Elasticsearch 8.0 Hardening Guide based on Application Server SRG V3R1

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must limit the number of concurrent sessions to an organization-defined number for all accounts and/or account types.
STIG ID: SRG-APP-000001 **Rule ID:** SV-204708r508029_rule **Vul ID:** V-204708
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation and configuration to determine if the number of concurrent sessions can be limited to the organization-defined number of sessions for all accounts and/or account types.

If a feature to limit the number of concurrent sessions is not available, is not set, or is set to unlimited, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using external Identity Provider (IdP) for authenticated user executes. Elasticsearch is a REST API and, as such, has no notion of sessions. Elasticsearch and Kibana do not have a connection limit.

To accomplish a connection limit, a proxy should be placed in front of the cluster.

For Elasticsearch as a SaaS product (Elastic-hosted), concurrent sessions are controlled further upstream via VPN Gateway limits (max connection of one per gateway) and by the use of Gravitational Teleport as an alternate gateway to Open SSH for managing access by Admins inside the production environment to clusters of Linux servers via SSH or the Kubernetes API.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application management includes the ability to control the number of sessions that utilize an application by all accounts and/or account types. Limiting the number of allowed sessions is helpful in limiting risks related to Denial of Service attacks.

Application servers host and expose business logic and application processes.

The application server must possess the capability to limit the maximum number of concurrent sessions in a manner that affects the entire application server or on an individual application basis.

Although there is some latitude concerning the settings themselves, the settings should follow DoD-recommended values, but the settings should be configurable to allow for future DoD direction.

While the DoD will specify recommended values, the values can be adjusted to accommodate the operational requirement of a given system.

Legacy Ids: V-35070; SV-46335

Comments:

CCI: CCI-000054 The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.NIST SP 800-53 :: AC-10NIST SP 800-53A :: AC-10.1 (ii)NIST SP 800-53 Revision 4 :: AC-10

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use encryption strength in accordance with the categorization of the management data during remote access management sessions.
STIG ID: SRG-APP-000014 **Rule ID:** SV-204709r508029_rule **Vul ID:** V-204709
Severity: CAT II

Documentable: No

Check Content:
Check the application server configuration to ensure all management interfaces use encryption in accordance with the management data.

If the application server is not configured to encrypt remote access management sessions in accordance with the categorization of the management data, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html

e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Remote management access is accomplished by leveraging common communication protocols and establishing a remote connection to the application server via a network for the purposes of managing the application server. If cryptography is not used, then the session data traversing the remote connection could be intercepted and compromised.

Types of management interfaces utilized by an application server include web-based HTTPS interfaces as well as command line-based management interfaces.

Legacy Ids: V-35089; SV-46376

Comments:

CCI: CCI-000068The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.NIST SP 800-53 :: AC-17 (2)NIST SP 800-53A :: AC-17 (2).1NIST SP 800-53 Revision 4 :: AC-17 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must implement cryptography mechanisms to protect the integrity of the remote access session.
STIG ID: SRG-APP-000015 **Rule ID:** SV-204710r508029_rule **Vul ID:** V-204710
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to ensure the application server is configured to use cryptography to protect the integrity of remote access sessions.

If the application server is not configured to implement cryptography mechanisms to protect the integrity of remote access sessions, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active

Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html

o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Encryption is critical for protection of remote access sessions. If encryption is not being used for integrity, malicious users may gain the ability to modify the application server configuration. The use of cryptography for ensuring integrity of remote access sessions mitigates that risk.

Application servers utilize a web management interface and scripted commands when allowing remote access. Web access requires the use of TLS and scripted access requires using ssh or some other form of approved cryptography. Application servers must have a capability to enable a secure remote admin capability.

FIPS 140-2 approved TLS versions must be enabled and non-FIPS-approved SSL versions must be disabled.

NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-35090; SV-46377

Comments:

CCI: CCI-001453The information system implements cryptographic mechanisms to protect the integrity of remote access sessions.NIST SP 800-53 :: AC-17 (2)NIST SP 800-53A :: AC-17 (2).1NIST SP 800-53 Revision 4 :: AC-17 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must ensure remote sessions for accessing security functions and security-relevant information are logged.
STIG ID: SRG-APP-000016 **Rule ID:** SV-204711r508029_rule **Vul ID:** V-204711
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation to determine if the application server logs remote administrative sessions.

If the application server does not log remote sessions for the admin user, then this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to log an event for each instance when the administrator accesses the system remotely.

1. Elasticsearch can preform audit logging. Enable the audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log an event for each instance when the administrator accesses the system remotely.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Logging must be utilized in order to track system activity, assist in diagnosing system issues, and provide evidence needed for forensic investigations post security incident.

Remote access by administrators requires that the admin activity be logged.

Application servers provide a web and command line-based remote management capability for managing the application server. Application servers must ensure that all actions related to administrative functionality such as application server configuration are logged.

Legacy Ids: V-57411; SV-71683

Comments:

CCI: CCI-000067The information system monitors remote access methods.NIST SP 800-53 :: AC-17 (1)NIST SP 800-53A :: AC-17 (1).1NIST SP 800-53 Revision 4 :: AC-17 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
STIG ID: SRG-APP-000033 **Rule ID:** SV-204712r508029_rule **Vul ID:** V-204712
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and configuration to determine if the system enforces authorization requirements for logical access to the system in accordance with applicable policy.

If the application server is not configured to utilize access controls or follow access control policies, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:
a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Strong access controls are critical to securing the application server. Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) must be employed by the application server to control access between users (or processes acting on behalf of users) and objects (e.g., applications, files, records, processes, application domains) in the application server.

Without stringent logical access and authorization controls, an adversary may have the ability, with very little effort, to compromise the application server and associated supporting infrastructure.

Legacy Ids: V-35738; SV-47025

Comments:

CCI: CCI-000213The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.NIST SP 800-53 :: AC-3NIST SP 800-53A :: AC-3.1NIST SP 800-53 Revision 4 :: AC-3

Rule Title: The application server management interface must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.
STIG ID: SRG-APP-000068 **Rule ID:** SV-204713r508029_rule **Vul ID:** V-204713
Severity: CAT II

Documentable: No

Check Content:
Review the application server management interface configuration to verify the application server is configured to display the Standard Mandatory DoD Notice and Consent Banner before granting access.

The banner must read:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

If the application server management interface does not display the banner or displays an unapproved banner, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch natively does not provide a GUI interface to display the DoD Notice. Kibana can be used as the front end, to perform this configuration. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to perform this configuration. The recommendation is to integrate Elasticsearch with these services to display the Standard Mandatory DoD Notice and Consent

Banner before granting access to the Application Server.

References:
a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers are required to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system management interface, providing privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance that states that:

(i) users are accessing a U.S. Government information system;
(ii) system usage may be monitored, recorded, and subject to audit;
(iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
(iv) the use of the system indicates consent to monitoring and recording.

System use notification messages can be implemented in the form of warning banners displayed when individuals log on to the information system.

System use notification is intended only for information system access including an

interactive logon interface with a human user, and is not required when an interactive interface does not exist.

Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Legacy Ids: V-35096; SV-46383

Comments:

CCI: CCI-000048The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.NIST SP 800-53 :: AC-8 aNIST SP 800-53A :: AC-8.1 (ii)NIST SP 800-53 Revision 4 :: AC-8 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server management interface must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.

STIG ID: SRG-APP-000069 **Rule ID:** SV-204714r508029_rule **Vul ID:** V-204714
Severity: CAT II

Documentable: No

Check Content:
Review application server management interface product documentation and configuration to determine that the logon banner can be displayed until the user takes action to acknowledge the agreement.

If the banner screen allows continuation to the application server without user interaction, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch natively does not provide a GUI interface to display the DoD Notice. Kibana can be used as the front end, to perform this configuration. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to perform this configuration. The recommendation is to integrate Elasticsearch with these services to retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.

References:
a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To establish acceptance of system usage policy, a click-through banner at the application server management interface logon is required. The banner shall prevent further activity on the application server unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35098; SV-46385

Comments:

CCI: CCI-000050The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.NIST SP 800-53 :: AC-8 bNIST SP 800-53A :: AC-8.1 (iii)NIST SP 800-53 Revision 4 :: AC-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.
STIG ID: SRG-APP-000080 **Rule ID:** SV-204715r508029_rule **Vul ID:** V-204715
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and server configuration to determine if the system does protect against an individual's (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by

non-repudiation.

If the application does not meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:
a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html
i. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Non-repudiation of actions taken is required in order to maintain application integrity. Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message.

Non-repudiation protects individuals against later claims by an author of not having authored

a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document.

Typical application server actions requiring non-repudiation will be related to application deployment among developers/users and administrative actions taken by admin personnel.

Legacy Ids: V-35135; SV-46422

Comments:

CCI: CCI-000166The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.NIST SP 800-53 :: AU-10NIST SP 800-53A :: AU-10.1NIST SP 800-53 Revision 4 :: AU-10

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: For application servers providing log record aggregation, the application server must compile log records from organization-defined information system components into a system-wide log trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail.
STIG ID: SRG-APP-000086 **Rule ID:** SV-204716r508029_rule **Vul ID:** V-204716
Severity: CAT II

Documentable: No

Check Content:
Review the application server log feature configuration to determine if the application server or an external logging tool in conjunction with the application server does compile log records from multiple components within the server into a system-wide log trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. All applications should capture the time of log/event creation.

Note: Elasticsearch architecture is designed to collect log records from multiple components within the server into a system-wide log trail.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.
date {
match =>; ...
time zone =>; "%{tz}"; # or whatever you call the field
}

4. To verify if the ingest pipeline is setup to capture the time, use the following: GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/8.0/add-locale.html
c. Processors:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest-processors.html
d. Ingest node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html
e. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/date-processor.html
f. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/get-pipeline-api.html
g. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
h. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
i. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log generation and log records can be generated from various components within the application server. The list of logged events is the set of events for which logs are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating log records (e.g., logable events, time stamps, source and

destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked).

The events occurring must be time-correlated in order to conduct accurate forensic analysis. In addition, the correlation must meet certain tolerance criteria. For instance, DoD may define that the time stamps of different logged events must not differ by any amount greater than ten seconds. It is also acceptable for the application server to utilize an external logging tool that provides this capability.

Legacy Ids: V-35139; SV-46426

Comments:

CCI: CCI-000174The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.NIST SP 800-53 :: AU-12 (1)NIST SP 800-53A :: AU-12 (1).1 (iii&v)NIST SP 800-53 Revision 4 :: AU-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records for access and authentication events.
STIG ID: SRG-APP-000089 **Rule ID:** SV-204717r508029_rule **Vul ID:** V-204717
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the deployed system configuration to determine if, at a minimum, system startup and shutdown, system access, and system authentication events are logged.

If the logs do not include the minimum logable events, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to generate log records for system startup and shutdown, system access, and system authentication events.

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.

Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log for system startup and shutdown, system access, and system authentication events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Starting Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/starting-elasticsearch.html
o. Stopping Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/stopping-elasticsearch.html
p. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
q. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html
r. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log records can be generated from various components within the application server. From an application server perspective, certain specific application server functionalities may be logged as well. The application server must allow the definition of what events are to be logged. As conditions change, the number and types of events to be logged may change, and the application server must be able to facilitate these changes.

The minimum list of logged events should be those pertaining to system startup and shutdown, system access, and system authentication events.

Legacy Ids: V-35141; SV-46428

Comments:

CCI: CCI-000169The information system provides audit record generation capability for the auditable events defined in AU-2 a at organization-defined information system components.NIST SP 800-53 :: AU-12 aNIST SP 800-53A :: AU-12.1 (ii)NIST SP 800-53 Revision 4 :: AU-12 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must allow only the ISSM (or individuals or roles appointed by the ISSM) to select which logable events are to be logged.

STIG ID: SRG-APP-000090 **Rule ID:** SV-204718r508029_rule **Vul ID:** V-204718
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and configuration to determine if the system only allows the ISSM (or individuals or roles appointed by the ISSM) to change logable events.

If the system is not configured to perform this function, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a specified format.

3. Recommend using an external Identity Management system for authentication of users. Then use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

4. If users are authenticated with the native or file realms, role assignment can be managed using the user management APIs or the users command-line tool (elasticsearch-users), respectively.

Role-mappings can be defined via an API or managed through files. These two sources of role-mapping are combined inside the Elasticsearch security features, so it is possible for a single user to have some Roles mapped through the API and other Roles mapped through files.

Role-mappings must be created for other types of realms that define which Roles should be assigned to each user based on their username, groups, or other metadata.

References:

a. Elasticsearch authentication:
https://www.elastic.co/blog/a-deep-dive-into-elasticsearch-authentication-realms
b. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
c. Role-based access control (RBAC) in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
d. Create or update role mappings API:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html

e. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
f. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
g. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
h. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
i. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
j. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
k. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
l. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
m. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
n. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
o. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
p. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
q. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
r. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
s. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log records can be generated from various components within the application server, (e.g., httpd, beans, etc.) From an application perspective, certain specific application functionalities may be logged, as well.

The list of logged events is the set of events for which logs are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating log records (e.g., logable events, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked).

Application servers utilize role-based access controls in order to specify the individuals who are allowed to configure application component logable events. The application server must be configured to select which personnel are assigned the role of selecting which logable events are to be logged.

The personnel or roles that can select logable events are only the ISSM (or individuals or roles appointed by the ISSM).

Legacy Ids: V-35142; SV-46429

Comments:

CCI: CCI-000171The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system.NIST SP 800-53 :: AU-12 bNIST SP 800-53A :: AU-12.1 (iii)NIST SP 800-53 Revision 4 :: AU-12 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful attempts to access subject privileges occur.
STIG ID: SRG-APP-000091 **Rule ID:** SV-204719r508029_rule **Vul ID:** V-204719
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when successful/unsuccessful attempts are made to access privileges.

If log records are not generated, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to generate log records when privileges are successfully/unsuccessfully accessed.

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at

https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log records when privileges are successfully/unsuccessfully accessed.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Accessing a subject's privileges can be used to elevate a lower-privileged subject's privileges temporarily in order to cause harm to the application server or to gain privileges to operate temporarily for a designed purpose. When these actions take place, the event needs to be logged.

Application servers either provide a local user store, or they integrate with enterprise user stores like LDAP. When the application server provides the user store and enforces authentication, the application server must generate a log record when modification of privileges is successfully or unsuccessfully performed.

Legacy Ids: V-35143; SV-46430

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must initiate session logging upon startup.
STIG ID: SRG-APP-000092 **Rule ID:** SV-204720r508029_rule **Vul ID:** V-204720
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation and server configuration to determine if the application server initiates session logging on application server startup.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. By enabling Set xpack.security.audit.enabled to true in elasticsearch.yml for each cluster node, Elastic starts up auditing when the node is started.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) which must be configured to initiate session logging upon startup.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Session logging activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Legacy Ids: V-35148; SV-46435

Comments:

CCI: CCI-001464The information system initiates session audits at system start-up.NIST SP 800-53 :: AU-14 (1)NIST SP 800-53A :: AU-14 (1).1NIST SP 800-53 Revision 4 :: AU-14 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing information to establish what type of events occurred.
STIG ID: SRG-APP-000095 **Rule ID:** SV-204721r508029_rule **Vul ID:** V-204721
Severity: CAT II

Documentable: No

Check Content:
Review the application server log configuration to determine if the application server produces log records showing what type of event occurred.

If the log data does not show the type of event, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish what type of events occurred. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
w. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Without being able to establish what type of event occurred, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible.

Log record content that may be necessary to satisfy the requirement of this control includes time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Application servers must log all relevant log data that pertains to the application server. Examples of relevant data include, but are not limited to, Java Virtual Machine (JVM) activity, HTTPD/Web server activity, and application server-related system process activity.

Legacy Ids: V-35159; SV-46446

Comments:

CCI: CCI-000130The information system generates audit records containing information that establishes what type of event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing sufficient information to establish when (date and time) the events occurred.
STIG ID: SRG-APP-000096 **Rule ID:** SV-204722r508029_rule **Vul ID:** V-204722
Severity: CAT II

Documentable: No

Check Content:
Review the logs on the application server to determine if the date and time are included in the log event data.

If the date and time are not included, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, @timestamp has to be captured.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish when the events occurred. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats

u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
w. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
x. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct order of the events that occurred is important during forensic analysis. Events that appear harmless by themselves might be flagged as a potential threat when properly viewed in sequence. By also establishing the event date and time, an event can be properly viewed with an enterprise tool to fully see a possible threat in its entirety.

Without sufficient information establishing when the log event occurred, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, file names involved, access control, or flow control rules invoked.

In addition to logging event information, application servers must also log the corresponding dates and times of these events. Examples of event data include, but are not limited to, Java Virtual Machine (JVM) activity, HTTPD activity, and application server-related system process activity.

Legacy Ids: V-35165; SV-46452

Comments:

CCI: CCI-000131The information system generates audit records containing information that establishes when an event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing sufficient information to establish where the events occurred.
STIG ID: SRG-APP-000097 **Rule ID:** SV-204723r508029_rule **Vul ID:** V-204723
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings on the application server to determine if the application server is configured to log information that establishes where within the application server the event occurred.

The data in the log file should identify the event, the component, module, filename, host name, servlets, containers, APIs, or other functionality within the application server, as well as, any source and destination information that indicates where an event occurred.

If the application server is not configured to log where within the application server the event took place, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, node.name, node.id, host.ip, host.name, origin.address, origin.type, has to be captured.

5. For event.type equal to transport, then extra attributes should be captured: action, indices, request.name

6. For event.type equal to ip_filter, transport_profile and rule should be captured.

7. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish where the events occurred. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct location or process within the application server where the events occurred is important during forensic analysis. To determine where an event occurred, the log data must contain information that identifies the source and destination of the events such as application components, modules, filenames, host names, servlets, containers, APIs, and other functionality.

Legacy Ids: V-35167; SV-46454

Comments:

CCI: CCI-000132The information system generates audit records containing information that establishes where the event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing sufficient information to establish the sources of the events.
STIG ID: SRG-APP-000098 **Rule ID:** SV-204724r508029_rule **Vul ID:** V-204724
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployment configuration to determine if the application server is configured to generate sufficient information to resolve the source, e.g., source IP, of the log event.

Request a user access the application server and generate logable events, and then review the logs to determine if the source of the event can be established.

If the source of the event cannot be determined, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, node.name, node.id, host.ip, host.name, origin.address, origin.type, has to be captured.

5. For event.type equal to transport, then extra attributes should be captured: action, indices, request.name

6. For event.type equal to ip_filter, transport_profile and rule should be captured.

7. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish the source of the events. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct source, e.g., source IP, of the events is important during forensic analysis. Correctly determining the source will add information to the overall reconstruction of the logable event. By determining the source of the event correctly, analysis of the enterprise can be undertaken to determine if the event compromised other assets within the enterprise.

Without sufficient information establishing the source of the logged event, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific

events, success/fail indications, file names involved, access control, or flow control rules invoked.

Legacy Ids: V-35170; SV-46457

Comments:

CCI: CCI-000133The information system generates audit records containing information that establishes the source of the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records that contain sufficient information to establish the outcome of events.
STIG ID: SRG-APP-000099 **Rule ID:** SV-204725r508029_rule **Vul ID:** V-204725
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and the log files on the application server to determine if the logs contain information that establishes the outcome of event data.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. event.action captures the type of event that occurred: anonymous_access_denied, authentication_failed, authentication_success, realm_authentication_failed, access_denied, access_granted, connection_denied, connection_granted, tampered_request, run_as_denied, or run_as_granted.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish the outcome of the events. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html

v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, filenames involved, access control or flow control rules invoked.

Success and failure indicators ascertain the outcome of a particular application server event or function. As such, they also provide a means to measure the impact of an event and help authorized personnel to determine the appropriate response. Event outcome may also include event-specific results (e.g., the security state of the information system after the event occurred).

Legacy Ids: V-35176; SV-46463

Comments:

CCI: CCI-000134The information system generates audit records containing information that establishes the outcome of the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records containing information that establishes the identity of any individual or process associated with the event.
STIG ID: SRG-APP-000100 **Rule ID:** SV-204726r508029_rule **Vul ID:** V-204726
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and the log files on the application server to determine if the logs contain information that establishes the identity of the user or process

associated with log event data.

If the application server does not produce logs that establish the identity of the user or process associated with log event data, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. event.action captures the type of event that occurred: anonymous_access_denied, authentication_failed, authentication_success, realm_authentication_failed, access_denied, access_granted, connection_denied, connection_granted, tampered_request, run_as_denied, or run_as_granted.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information that establishes the identity of any individual or process associated with the event. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes: time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Application servers have differing levels of logging capabilities that can be specified by setting a verbosity level. The application server must, at a minimum, be capable of establishing the identity of any user or process that is associated with any particular event.

Legacy Ids: V-35182; SV-46469

Comments:

CCI: CCI-001487The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records containing the full-text recording of privileged commands or the individual identities of group account users.
STIG ID: SRG-APP-000101 **Rule ID:** SV-204727r508029_rule **Vul ID:** V-204727
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployment configuration to determine if the application server is configured to generate full-text recording of privileged commands or the individual identities of group users at a minimum.

Have a user execute a privileged command and review the log data to validate that the full-text or identity of the individual is being logged.

If the application server is not meeting this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. Configure the log ingestion pipeline including Logstash/Beats to generate log records

containing the full-text recording of privileged commands or the individual identities of group account users. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Privileged commands are commands that change the configuration or data of the application server. Since this type of command changes the application server configuration and could possibly change the security posture of the application server, these commands need to be logged to show the full-text of the command executed. Without the full-text, reconstruction of harmful events or forensic analysis is not possible.

Organizations can consider limiting the additional log information to only that information explicitly needed for specific log requirements. At a minimum, the organization must log either full-text recording of privileged commands or the individual identities of group users, or both. The organization must maintain log trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Legacy Ids: V-57417; SV-71689

Comments:

CCI: CCI-000135The information system generates audit records containing the organization-defined additional

CCI: more detailed information that is to be included in the audit records.NIST SP 800-53 :: AU-3 (1)NIST SP 800-53A :: AU-3 (1).1 (ii)NIST SP 800-53 Revision 4 :: AU-3 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must alert the SA and ISSO, at a minimum, in the event of a log processing failure.
STIG ID: SRG-APP-000108 **Rule ID:** SV-204728r508029_rule **Vul ID:** V-204728
Severity: CAT II

Documentable: No

Check Content:
Review application server log configuration. Verify the application server sends alerts to the SA and ISSO in the event of a log processing failure.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:

Steps/Recommendation:

Recommend establishing an alert for SA and ISSO, at a minimum, that triggers in the event of a log processing failure.

1. The Elastic Stack API can be used to setup alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Kibana Alerts
The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify you of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. However, they can be tailored to meet the organization needs.

Missing monitoring data:
This alert is triggered when any stack product nodes or instances stop sending monitoring data. By default, the trigger condition is set to missing for 15 minutes looking back 1 day. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 6 hours.

References:

a. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/how-monitoring-works.html
b. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
c. Kibana Alerts: https://www.elastic.co/guide/en/kibana/8.0/kibana-alerts.html
d. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/collecting-monitoring-data.html
e. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
f. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
g. cat nodes API: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-nodes.html
h. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Logs are essential to monitor the health of the system, investigate changes that occurred to the system, or investigate a security incident. When log processing fails, the events during the failure can be lost. To minimize the timeframe of the log failure, an alert

needs to be sent to the SA and ISSO at a minimum.

Log processing failures include, but are not limited to, failures in the application server log capturing mechanisms or log storage capacity being reached or exceeded. In some instances, it is preferred to send alarms to individuals rather than to an entire group. Application servers must be able to trigger an alarm and send an alert to, at a minimum, the SA and ISSO in the event there is an application server log processing failure.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35186; SV-46473

Comments:

CCI: CCI-000139The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.NIST SP 800-53 :: AU-5 aNIST SP 800-53A :: AU-5.1 (ii)NIST SP 800-53 Revision 4 :: AU-5 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must shut down by default upon log failure (unless availability is an overriding concern).
STIG ID: SRG-APP-000109 **Rule ID:** SV-204729r508029_rule **Vul ID:** V-204729
Severity: CAT II

Documentable: No

Check Content:
If the application server is a high availability system, this finding is NA.

Review the application server configuration settings to determine if the application server is configured to shut down on a log failure.

If the application server is not configured to shut down on a log failure, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch will go into a read-only state when it detects issues with disk storage which is the most common issue affecting logging. Elasticsearch will not shutdown if logging fails for

other reasons.

Elasticsearch should be configured so as to continue to log but cache the logs locally until log shipment can resume. Capacity of the disk receiving logs is generally the issue that causes this sort of failure. Availability is generally an overriding concern, so rather than shutting down when the log shipping fails, local caching should be used to keep the system available and permit "catching up" on log shipment once the issue is resolved. Per NIST 800-53, it is preferable to overwrite logs rather than shut down logging if there is no other option. Also recommend establishing an alert that triggers when logs fail to ship after collection for any reason, so the issue can be detected and resolved in a timely manner, before overwriting must be used as a measure of last resort to keep the system available.

2. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Returns information about a cluster’s nodes.
Request
GET /_cat/nodes

disk.total, dt, diskTotal
Total disk space, such as 458.3gb.
disk.used, du, diskUsed
Used disk space, such as 259.8gb.
disk.avail, d, disk, diskAvail
Available disk space, such as 198.4gb.
disk.used_percent, dup, diskUsedPercent
Used disk space percentage, such as 47.

3. Kibana Alerts: The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify you of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. However, you can tailor them to meet your specific needs.

Missing monitoring data:
This alert is triggered when any stack products nodes or instances stop sending monitoring data. By default, the trigger condition is set to missing for 15 minutes looking back 1 day. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 6 hours.

Disk usage threshold:
This alert is triggered when a node is nearly at disk capacity. By default, the trigger condition is set at 80% or more averaged over the last 5 minutes. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 1 day.

References:

a. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/how-monitoring-works.html
b. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
c. Kibana Alerts: https://www.elastic.co/guide/en/kibana/8.0/kibana-alerts.html
d. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/collecting-monitoring-data.html
e. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
f. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
g. cat nodes API: https:/hwww.elastic.co/guide/en/elasticsearch/reference/8.0/cat-nodes.html
h. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical that, when a system is at risk of failing to process logs, it detects and takes action to mitigate the failure. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. During a failure, the application server must be configured to shut down unless the application server is part of a high availability system.

When availability is an overriding concern, other approved actions in response to a log failure are as follows:

(i) If the failure was caused by the lack of log record storage capacity, the application must continue generating log records if possible (automatically restarting the log service if necessary), overwriting the oldest log records in a first-in-first-out manner.

(ii) If log records are sent to a centralized collection server and communication with this server is lost or the server fails, the application must queue log records locally until communication is restored or until the log records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local log data with the collection server.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35190; SV-46477

Comments:

CCI: CCI-000140The information system takes organization-defined actions upon audit failure (e.g.) shut down information system, overwrite oldest audit records stop generating audit records).NIST SP 800-53 :: AU-5 bNIST SP 800-53A :: AU-5.1 (iv)NIST SP 800-53 Revision 4 :: AU-5 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured to fail over to another system in the event of log subsystem failure.
STIG ID: SRG-APP-000109 **Rule ID:** SV-204730r508029_rule **Vul ID:** V-204730
Severity: CAT II

Documentable: No

Check Content:
If the system MAC level and availability do not require redundancy, this requirement is NA.

Review the system's accreditation documentation to determine system MAC and confidentiality requirements. Review application server configuration settings to determine if the application server is configured to fail over operation to another system when the log subsystem fails to operate.

If the system MAC level requires redundancy and the application server is not configured to fail over to another system which can handle application and log functions when a log subsystem failure occurs, this is a finding.

Fix Text:
Steps/Recommendation:

If the system MAC level and availability do not require redundancy, this requirement is NA.

1. Elasticsearch provides a clustering capability by design and can be configured in a high-availability (HA) cluster. Elasticsearch offers a number of features to achieve HA despite failures.

- With proper planning, a cluster can be designed for resilience to many of the things that commonly go wrong, from the loss of a single node or network connection right up to a zone-wide outage such as power loss.

- Enable cross-cluster replication to replicate data to a remote follower cluster which may be in a different data centre or even on a different continent from the leader cluster. The follower cluster acts as a hot standby, ready to fail over in the event of a disaster so severe that the leader cluster fails. The follower cluster can also act as a geo-replica to serve searches from nearby clients.
- The last line of defense against data loss is to take regular snapshots of the cluster so that a copy can be restored elsewhere if needed.

Designing for resilience
A resilient cluster requires redundancy for every required cluster component. This means a resilient cluster must have:
- At least three master-eligible nodes
- At least two nodes of each role
- At least two copies of each shard (one primary and one or more replicas)

Back up a cluster:
WARNING: An Elasticsearch cluster cannot be backed up simply by copying the data directories of all of its nodes. Elasticsearch may be making changes to the contents of its data directories while it is running; copying its data directories cannot be expected to capture a consistent picture of their contents. If restoring a cluster from such a backup, it may fail and report corruption and/or missing files. Alternatively, it may appear to have succeeded though it silently lost some of its data. The only reliable way to back up a cluster is by using the snapshot and restore functionality.

To have a complete backup for a cluster:
- Back up the data
- Back up the cluster configuration
- Back up the security configuration

2. If using Elasticsearch as a SaaS product (Elastic-hosted), recommend a minimum of three availability zones to enable Elastic Cloud Enterprise to create clusters with a tiebreaker.

High availability
- Fault tolerance for Elastic Cloud Enterprise is based around the concept of availability zones.
- An availability zone contains resources available to an Elastic Cloud Enterprise installation that are isolated from other availability zones to safeguard against potential failure.
- If there are only two availability zones in total in the installation, no tiebreaker is created.

3. Refer to the cloud provider options of Regions and Availability Zones for high-availability (HA) cluster for hosting the Elastic cluster.

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html

b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html
c. Set up a cluster for high availability:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability.html
d. Designing for resilience:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability-cluster-design.html
e. Cross-cluster replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html
f. Back up a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/backup-cluster.html
g. High availability: https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-ha.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This requirement is dependent upon system MAC and availability. If the system MAC and availability do not specify redundancy requirements, this requirement is NA.

It is critical that, when a system is at risk of failing to process logs as required, it detects and takes action to mitigate the failure.

Application servers must be capable of failing over to another system which can handle application and logging functions upon detection of an application log processing failure. This will allow continual operation of the application and logging functions while minimizing the loss of operation for the users and loss of log data.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35191; SV-46478

Comments:

CCI: CCI-000140The information system takes organization-defined actions upon audit failure (e.g. shut down information system overwrite oldest audit records stop generating audit records).NIST SP 800-53 :: AU-5 bNIST SP 800-53A :: AU-5.1 (iv)NIST SP 800-53 Revision 4 :: AU-5 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use internal system clocks to generate time stamps for log records.
STIG ID: SRG-APP-000116 **Rule ID:** SV-204731r508029_rule **Vul ID:** V-204731
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration files to determine if the internal system clock is used for time stamps. If this is not feasible, an alternative workaround is to take an action that generates an entry in the logs and then immediately query the operating system for the current time. A reasonable match between the two times will suffice as evidence that the system is using the internal clock for timestamps.

If the application server does not use the internal system clock to generate time stamps, this is a finding.

Fix Text:
Steps/Recommendation:

1. All applications should capture the time of log/event creation.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Recommended to setup NTP or Chrony in all host to avoid time drift in servers.

4. To verify if the ingest pipeline is setup to capture the time, use the following: GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. Processors:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest-processors.html
b. Ingest Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html
c. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/date-processor.html
d. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/get-pipeline-api.html
e. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
f. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html

g. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/8.0/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without the use of an approved and synchronized time source configured on the systems, events cannot be accurately correlated and analyzed to determine what is transpiring within the application server.

If an event has been triggered on the network, and the application server is not configured with the correct time, the event may be seen as insignificant, when in reality the events are related and may have a larger impact across the network. Synchronization of system clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. Determining the correct time a particular event occurred on a system, via time stamps, is critical when conducting forensic analysis and investigating system events.

Application servers must utilize the internal system clock when generating time stamps and log records.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35203; SV-46490

Comments:

CCI: CCI-000159The information system uses internal system clocks to generate time stamps for audit records.NIST SP 800-53 :: AU-8NIST SP 800-53A :: AU-8.1NIST SP 800-53 Revision 4 :: AU-8 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log information from any type of unauthorized read access.
STIG ID: SRG-APP-000118 **Rule ID:** SV-204732r508029_rule **Vul ID:** V-204732
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log features protect log information from unauthorized access.

Review file system settings to verify the application server sets secure file permissions on log files.

If the application server does not protect log information from unauthorized read access, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized access with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to Elasticsearch cluster with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If log data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve. In addition, access to log records provides information an attacker could potentially use to his or her advantage.

Application servers contain admin interfaces that allow reading and manipulation of log records. Therefore, these interfaces should not allow unfettered access to those records. Application servers also write log data to log files which are stored on the OS, so appropriate file permissions must also be used to restrict access.

Log information includes all information (e.g., log records, log settings, transaction logs, and log reports) needed to successfully log information system activity. Application servers must protect log information from unauthorized read access.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35205; SV-46492

Comments:

CCI: CCI-000162The information system protects audit information from unauthorized access.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log information from unauthorized modification.
STIG ID: SRG-APP-000119 **Rule ID:** SV-204733r508029_rule **Vul ID:** V-204733
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log features protect log information from unauthorized modification.

Review file system settings to verify the application server sets secure file permissions on log files to prevent unauthorized modification.

If the application server does not protect log information from unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized modification with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If log data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve. In addition, access to log records provides information an attacker could potentially use to his or her advantage.

Application servers contain admin interfaces that allow reading and manipulation of log records. Therefore, these interfaces should not allow unfettered access to those records. Application servers also write log data to log files which are stored on the OS, so appropriate file permissions must also be used to restrict access.

Log information includes all information (e.g., log records, log settings, transaction logs and log reports) needed to successfully log information system activity. Application servers must protect log information from unauthorized modification.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35772; SV-47059

Comments:

CCI: CCI-000163The information system protects audit information from unauthorized modification.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log information from unauthorized deletion.
STIG ID: SRG-APP-000120 **Rule ID:** SV-204734r508029_rule **Vul ID:** V-204734
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log features protect log information from unauthorized deletion.

Review file system settings to verify the application server sets secure file permissions on log files to prevent unauthorized deletion.

If the application server does not protect log information from unauthorized deletion, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized deletion with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between

Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If log data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve.

Application servers contain admin interfaces that allow reading and manipulation of log records. Therefore, these interfaces should not allow for unfettered access to those records. Application servers also write log data to log files which are stored on the OS, so appropriate file permissions must also be used to restrict access.

Log information includes all information (e.g., log records, log settings, transaction logs, and log reports) needed to successfully log information system activity. Application servers must protect log information from unauthorized deletion.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35212; SV-46499

Comments:

CCI: CCI-000164The information system protects audit information from unauthorized deletion.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log tools from unauthorized access.
STIG ID: SRG-APP-000121 **Rule ID:** SV-204735r508029_rule **Vul ID:** V-204735
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and server configuration to determine if the application server protects log tools from unauthorized access.

Request a system administrator attempt to access log tools while logged into the server in a role that does not have the requisite privileges.

If the application server does not protect log tools from unauthorized access, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized access with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to Elasticsearch cluster with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html

d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting log data also includes identifying and protecting the tools used to view and manipulate log data.

Depending upon the log format and application, system and application log tools may provide the only means to manipulate and manage application and system log data.

It is, therefore, imperative that access to log tools be controlled and protected from unauthorized access.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected as well.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35213; SV-46500

Comments:

CCI: CCI-001493The information system protects audit tools from unauthorized access.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log tools from unauthorized modification.

STIG ID: SRG-APP-000122 **Rule ID:** SV-204736r508029_rule **Vul ID:** V-204736
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and server configuration to determine if the application server protects log tools from unauthorized modification. Request a system administrator attempt to modify log tools while logged into the server in a role that does not have the requisite privileges.

Locate binary copies of log tool executables that are located on the file system and attempt to modify using unprivileged credentials.

If the application server does not protect log tools from unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized modification with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting log data also includes identifying and protecting the tools used to view and manipulate log data.

Depending upon the log format and application, system and application log tools may provide the only means to manipulate and manage application and system log data.

It is, therefore, imperative that access to log tools be controlled and protected from unauthorized modification. If an attacker were to modify log tools, he could also manipulate logs to hide evidence of malicious activity.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected as well.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35214; SV-46501

Comments:

CCI: CCI-001494The information system protects audit tools from unauthorized modification.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log tools from unauthorized deletion.
STIG ID: SRG-APP-000123 **Rule ID:** SV-204737r508029_rule **Vul ID:** V-204737
Severity: CAT II

Documentable: No

Check Content:

Review the application server documentation and server configuration to determine if the application server protects log tools from unauthorized deletion.

Locate binary copies of log tool executables that are located on the file system and attempt to delete using unprivileged credentials.

If the application server does not protect log tools from unauthorized deletion, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized deletion with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting log data also includes identifying and protecting the tools used to view and manipulate log data.

Depending upon the log format and application, system and application log tools may provide

the only means to manipulate and manage application and system log data.

It is, therefore, imperative that access to log tools be controlled and protected from unauthorized modification. If an attacker were to delete log tools, the application server administrator would have no way of managing or viewing the logs.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar, class or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected from unauthorized deletion as well.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35215; SV-46502

Comments:

CCI: CCI-001495The information system protects audit tools from unauthorized deletion.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must back up log records at least every seven days onto a different system or system component than the system or component being logged.
STIG ID: SRG-APP-000125 **Rule ID:** SV-204738r508029_rule **Vul ID:** V-204738
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server backs up log records every seven days onto a different system or media from the system being logged.

If the application server does not back up log records every seven days onto a different system or media from the system being logged, this is a finding.

Fix Text:
Steps/Recommendation:

1. Setup appropriate lifecycle for the indices and create snapshots.

2. Elasticsearch can be configured to provide redundancy by storing the Elasticsearch data into a different system or system component than the system or component being logged.

References:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/8.0/resiliency.html
b. Manage the index lifecycle:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-lifecycle-management.html
c. Configure snapshot lifecycle policies:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/getting-started-snapshot-lifecycle-management.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protection of log data includes assuring log data is not accidentally lost or deleted. Backing up log records to a different system or onto separate media from the system the application server is actually running on helps to assure that in the event of a catastrophic system failure, the log records will be retained.

Legacy Ids: V-35216; SV-46503

Comments:

CCI: CCI-001348The information system backs up audit records on an organization-defined frequency onto a different system or system component than the system or component being audited.NIST SP 800-53 :: AU-9 (2)NIST SP 800-53A :: AU-9 (2).1 (iii)NIST SP 800-53 Revision 4 :: AU-9 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use cryptographic mechanisms to protect the integrity of log information.
STIG ID: SRG-APP-000126 **Rule ID:** SV-204739r508029_rule **Vul ID:** V-204739
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server can be configured to protect the integrity of log data using cryptographic hashes and digital signatures. Configure the application server to hash and sign log data. This is typically done the moment when log files cease to be written to and are rolled over for storage or offloading.

Alternatively, if the application server is not able to hash and sign log data, the task can be delegated by configuring the application server or underlying OS to send logs to a centralized log management system or SIEM that can meet the requirement.

If the application server is not configured to hash and sign logs, or is not configured to utilize the aforementioned OS and centralized log management resources to meet the requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. For the Elastic cloud hosted service offerings, Elastic uses Auditbeat and Elastic Endpoint Security as host-based intrusion detection system and File Integrity Management (HIDS)/(FIM) on all hosts, specifying files and directories to be monitored for changes. File changes are detected in near real time and sent to Elasticsearch clusters in the Security Control Plane with metadata and cryptographic hashes of the file to enable further analysis. If unauthorized changes or anomalous connections are detected in the AWS infrastructure, an alert is generated from the Elasticsearch clusters to notify the Information Security team of an anomalous event.

2. For an on-premise Elasticsearch deployment, it is recommended that a third party HIDS/FIM be implemented as a risk reduction method for this control.

References:

a. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
b. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: Protecting the integrity of log records helps to ensure log files are not tampered with. Cryptographic mechanisms are the industry-established standard used to protect the integrity of log data. An example of cryptographic mechanisms is the computation and application of a cryptographic hash and using asymmetric cryptography with digital signatures. Application Servers often write log data to files on the file system. These files typically roll over on a periodic basis. Once the logs are rolled over, hashing and signing the logs assures the logs are not tampered with and helps to assure log integrity.

Legacy Ids: V-35217; SV-46504

Comments:

CCI: CCI-001350The information system implements cryptographic mechanisms to protect the integrity of audit information.NIST SP 800-53 :: AU-9 (3)NIST SP 800-53A :: AU-9 (3).1NIST SP 800-53 Revision 4 :: AU-9 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.
STIG ID: SRG-APP-000131 **Rule ID:** SV-204740r508029_rule **Vul ID:** V-204740
Severity: CAT II

Documentable: No

Check Content:
Review system documentation to determine if the application server prevents the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, the Elasticsearch system does not prevent the installation of patches, service packs, or application components without verifying the software component has been digitally signed using a certificate that is recognized and approved by the organization.

Configure the operating system to verify the signature of local packages prior to install with a certificate recognized and approved by an organizationally maintained certificate authority.

2. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to verify the signature of packages prior to install of patches, service packs, or application components with a certificate recognized and approved by the an organizationally maintained certificate authority. Self-signed certificates are disallowed by this requirement.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Changes to any software components can have significant effects on the overall security of the application. Verifying software components have been digitally signed using a certificate that is recognized and approved by the organization ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, or application components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The application should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Legacy Ids: V-57495; SV-71771

Comments:

CCI: CCI-001749The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.NIST SP 800-53 Revision 4 :: CM-5 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must limit privileges to change the software resident within software libraries.
STIG ID: SRG-APP-000133 **Rule ID:** SV-204741r508029_rule **Vul ID:** V-204741
Severity: CAT II

Documentable: No

Check Content:
Check the application server documentation and configuration to determine if the application server provides role-based access that limits the capability to change shared software libraries.

Validate file permission settings to ensure library files are secured in relation to OS access.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1.For on premises implementation, the Elasticsearch system does not prevent modifications on the software resident within software libraries.

Configure the application OS file permissions to restrict access to software libraries and configure the application to restrict user access regarding software library update functionality to only authorized users or processes. For example, the Elasticsearch directory contents include among others:
LICENSE.txt, NOTICE.txt, README.asciidoc, bin, config, data, jdk, lib, logs, modules, plugins

Recommend establishing an alert for detecting such system changes so they can be evaluated promptly. For the hosted Elasticsearch Service (SaaS offering), only an Elastic Admin with access to the Infrastructure as Code files would be able to modify files and modules that cannot be configured directly by Customer. Customer is responsible for secure configuration with Role-based access control (RBAC) controls. Elastic monitors for such changes in the hosted production environment and investigates if detected.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers have the ability to specify that the hosted applications utilize shared libraries. The application server must have a capability to divide roles based upon duties wherein one project user (such as a developer) cannot modify the shared library code of another project user. The application server must also be able to specify that non-privileged users cannot modify any shared library code at all.

Legacy Ids: V-35224; SV-46511

Comments:

CCI: CCI-001499The organization limits privileges to change software resident within software libraries.NIST SP 800-53 :: CM-5 (6)NIST SP 800-53A :: CM-5 (6).1NIST SP 800-53 Revision 4 :: CM-5 (6)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be capable of reverting to the last known good configuration in the event of failed installations and upgrades.
STIG ID: SRG-APP-000133 **Rule ID:** SV-204742r508029_rule **Vul ID:** V-204742
Severity: CAT II

Documentable: No

Check Content:
Check the application server documentation and configuration to determine if the application server provides an automated rollback capability to a known good configuration in the event of a failed installation and upgrade.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. As part of the hosted Elasticsearch Service offering, customers may configure how they wish to run backups to enable rollback or restore of their configurations. Elastic is responsible

for SaaS and system wide capabilities for snapshot and restore operations at the SaaS layer level. Use of ECE, ECK, or Elastic Cloud is recommended; rollback is not supported by Elastic for "self-managed" implementations.

ECE supports rolling upgrades on an Elasticsearch cluster to be upgraded one node at a time so upgrading does not interrupt service.

2. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to enable rollback or restore to the last known good configuration in the event of failed installations and upgrades.

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Rolling upgrades:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/rolling-upgrades.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Any changes to the components of the application server can have significant effects on the overall security of the system.

In order to ensure a prompt response to failed application installations and application server upgrades, the application server must provide an automated rollback capability that allows the system to be restored to a previous known good configuration state prior to the application installation or application server upgrade.

Legacy Ids: V-57497; SV-71773

Comments:

CCI: CCI-001499The organization limits privileges to change software resident within software libraries.NIST SP 800-53 :: CM-5 (6)NIST SP 800-53A :: CM-5 (6).1NIST SP 800-53 Revision 4 :: CM-5 (6)

Rule Title: The application server must adhere to the principles of least functionality by providing only essential capabilities.
STIG ID: SRG-APP-000141 **Rule ID:** SV-204743r508029_rule **Vul ID:** V-204743
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server can disable non-essential features and capabilities.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. All audit logging requirements can be configured in elasticsearch.yml. The audit requirement should be defined by the line of business in the system security plan document. The configuration should match all the required audit attributes defined in the system security plan document.

2. To enable the required attributes as defined in the document, refer to latest documentation for full set of supported attributes:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

3. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts which need to be secured to match all the required audit attributes defined in the system security plan document.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html

h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers provide a myriad of differing processes, features and functionalities. Some of these processes may be deemed to be unnecessary or too unsecure to run on a production DoD system. Application servers must provide the capability to disable or deactivate functionality and services that are deemed to be non-essential to the server mission or can adversely impact server performance, for example, disabling dynamic JSP reloading on production application servers as a best practice.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35234; SV-46521

Comments:

CCI: CCI-000381The organization configures the information system to provide only essential capabilities.NIST SP 800-53 :: CM-7NIST SP 800-53A :: CM-7.1 (ii)NIST SP 800-53 Revision 4 :: CM-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prohibit or restrict the use of nonsecure ports, protocols, modules, and/or services as defined in the PPSM CAL and vulnerability assessments.
STIG ID: SRG-APP-000142 **Rule ID:** SV-204744r508029_rule **Vul ID:** V-204744
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployment configuration to determine which ports and protocols are enabled.

Verify that the ports and protocols being used are not prohibited and are necessary for the operation of the application server and the hosted applications.

If any of the ports or protocols is prohibited or not necessary for the application server operation, this is a finding.

Fix Text:
Steps/Recommendation:

1. Ensure all available ports are registered with PPSM.

2. Each Elasticsearch node has two different network interfaces. Clients send requests to Elasticsearch's REST APIs using its HTTP interface, but nodes communicate with other nodes using the transport interface. The transport interface is also used for communication with remote clusters.

The network settings described above apply to both methods of communication, and you can also configure each interface separately if needed.

3. The following settings can be configured for HTTP in elasticsearch.yml. By default, Elasticsearch runs on 9200 port. These settings also use the common network settings.

http.port
(Static) A bind port range. Defaults to 9200-9300.
http.publish_port
(Static) The port that HTTP clients should use when communicating with this node. Useful when a cluster node is behind a proxy or firewall and the http.port is not directly addressable from the outside. Defaults to the actual port assigned via http.port.
http.bind_host
(Static) The host address to bind the HTTP service to. Defaults to http.host (if set) or network.bind_host.
http.publish_host
(Static) The host address to publish for HTTP clients to connect to. Defaults to http.host (if set) or network.publish_host.
http.host
(Static) Used to set the http.bind_host and the http.publish_host.

4. The following settings can be configured for the internal transport that communicates over TCP in elasticsearch.yml.

The transport layer is used for all internal communication between nodes within a cluster, all communication with the nodes of a remote cluster, and also by the TransportClient in the Elasticsearch Java API.

Transport settings
Some of the available settings are presented below for brevity.

transport.port
(Static) A bind port range. Defaults to 9300-9400.
transport.publish_port
(Static) The port that other nodes in the cluster should use when communicating with this node. Useful when a cluster node is behind a proxy or firewall and the transport.port is not directly addressable from the outside. Defaults to the actual port assigned via transport.port.
transport.bind_host
(Static) The host address to bind the transport service to. Defaults to transport.host (if set) or network.bind_host.
transport.publish_host
(Static) The host address to publish for nodes in the cluster to connect to. Defaults to transport.host (if set) or network.publish_host.
transport.host

References:

a. DoD ports and protocols PPSM web site: https://public.cyber.mil/connect/ppsm/
b. HTTP:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-http.html#_http_settings
c. Configuring Elasticsearch Transport:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-transport.html
d. Network settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-network.html
e. ECE Networking:
https://www.elastic.co/guide/en/cloud-enterprise/2.6/ece-prereqs-networking.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Some networking protocols may not meet organizational security requirements to protect data and components.

Application servers natively host a number of various features, such as management interfaces, httpd servers and message queues. These features all run on TCP/IP ports. This

creates the potential that the vendor may choose to utilize port numbers or network services that have been deemed unusable by the organization. The application server must have the capability to both reconfigure and disable the assigned ports without adversely impacting application server operation capabilities. For a list of approved ports and protocols, reference the DoD ports and protocols web site at https://public.cyber.mil/connect/ppsm/

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57501; SV-71777

Comments:

CCI: CCI-000382The organization configures the information system to prohibit or restrict the use of organization defined functions ports, protocols and/or services.NIST SP 800-53 :: CM-7NIST SP 800-53A :: CM-7.1 (iii)NIST SP 800-53 Revision 4 :: CM-7 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use an enterprise user management system to uniquely identify and authenticate users (or processes acting on behalf of organizational users).
STIG ID: SRG-APP-000148 **Rule ID:** SV-204745r508029_rule **Vul ID:** V-204745
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server is using an enterprise solution to authenticate organizational users and processes running on the users' behalf.

If an enterprise solution is not being used, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with these services to uniquely identify and

authenticate users (or processes acting on behalf of organizational users).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure accountability and prevent unauthorized access, application server users must be uniquely identified and authenticated. This is typically accomplished via the use of a user store which is either local (OS-based) or centralized (LDAP) in nature.

To ensure support to the enterprise, the authentication must utilize an enterprise solution.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35299; SV-46586

Comments:

CCI: CCI-000764The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).NIST SP 800-53 :: IA-2NIST SP 800-53A :: IA-2.1NIST SP 800-53 Revision 4 :: IA-2

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use multifactor authentication for network access to privileged accounts.
STIG ID: SRG-APP-000149 **Rule ID:** SV-204746r508029_rule **Vul ID:** V-204746
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to ensure the system is authenticating via multifactor authentication for privileged users.

If all aspects of application server web management interfaces are not authenticating privileged users via multifactor authentication methods, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using an external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm enforce to ensure the system is authenticating via multifactor authentication for privileged users.

2. On hosted Elasticsearch Service (SaaS offering), follow the steps to enable multi-factor authentication:
To enable multi-factor authentication, you must enroll your device.

- Log in to the Elasticsearch Service Console.
- Go to Settings.
- Click Configure to enable the Authenticator app or Add a phone number to enable the Text message.

References:

a. Enable multi-factor authentication:
https://www.elastic.co/guide/en/cloud/current/ec-account-user-settings.html#ec-account-secur

ity-mfa
b. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
d. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
e. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
f. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
g. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
h. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
i. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Multifactor authentication creates a layered defense and makes it more difficult for an unauthorized person to access the application server. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Unlike a simple username/password scenario where the attacker could gain access by knowing both the username and password without the user knowing his account was compromised, multifactor authentication adds the requirement that the attacker must have something from the user, such as a token, or to biometrically be the user.

Multifactor authentication is defined as: using two or more factors to achieve authentication.

Factors include:
(i) something a user knows (e.g., password/PIN);
(ii) something a user has (e.g., cryptographic identification device, token); or
(iii) something a user is (e.g., biometric). A CAC or PKI Hardware Token meets this definition.

A privileged account is defined as an information system account with authorizations of a privileged user. These accounts would be capable of accessing the web management interface.

When accessing the application server via a network connection, administrative access to the

application server must be PKI Hardware Token enabled.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35300; SV-46587

Comments:

CCI: CCI-000765The information system implements multifactor authentication for network access to privileged accounts.NIST SP 800-53 :: IA-2 (1)NIST SP 800-53A :: IA-2 (1).1NIST SP 800-53 Revision 4 :: IA-2 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use multifactor authentication for local access to privileged accounts.
STIG ID: SRG-APP-000151 **Rule ID:** SV-204747r508029_rule **Vul ID:** V-204747
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to ensure the system is authenticating via multifactor authentication for privileged users.

If all aspects of application server command line management interfaces are not authenticating privileged users via multifactor authentication methods, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using an external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm enforce to ensure the system is authenticating via multifactor authentication for privileged users.

2. On hosted Elasticsearch Service (SaaS offering), follow the steps to enable multi-factor authentication:
To enable multi-factor authentication, you must enroll your device.
- Log in to the Elasticsearch Service Console.
- Go to Settings.

- Click Configure to enable the Authenticator app or Add a phone number to enable the Text message.

References:

a. Enable multi-factor authentication:
https://www.elastic.co/guide/en/cloud/current/ec-account-user-settings.html#ec-account-security-mfa
b. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
d. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
e. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
f. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
g. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
h. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
i. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Multifactor authentication creates a layered defense and makes it more difficult for an unauthorized person to access the application server. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Unlike a simple username/password scenario where the attacker could gain access by knowing both the username and password without the user knowing his account was compromised, multifactor authentication adds the requirement that the attacker must have something from the user, such as a token, or to biometrically be the user.

Multifactor authentication is defined as: using two or more factors to achieve authentication.

Factors include:

(i) something a user knows (e.g., password/PIN);
(ii) something a user has (e.g., cryptographic identification device, token); or
(iii) something a user is (e.g., biometric). A CAC or PKI Hardware Token meets this definition.

A privileged account is defined as an information system account with authorizations of a privileged user. These accounts would be capable of accessing the command line management interface.

When accessing the application server via a network connection, administrative access to the application server must be PKI Hardware Token enabled.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35301; SV-46588

Comments:

CCI: CCI-000767The information system implements multifactor authentication for local access to privileged accounts.NIST SP 800-53 :: IA-2 (3)NIST SP 800-53A :: IA-2 (3).1NIST SP 800-53 Revision 4 :: IA-2 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must authenticate users individually prior to using a group authenticator.
STIG ID: SRG-APP-000153 **Rule ID:** SV-204748r508029_rule **Vul ID:** V-204748
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server individually authenticates users prior to authenticating via a role or group.

Review application server logs to verify user accesses requiring authentication can be traced back to an individual account.

If the application server does not authenticate users on an individual basis, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with these services to authenticate users individually prior to using a group authenticator.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure individual accountability and prevent unauthorized access, application server users (and any processes acting on behalf of application server users) must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users.

Application servers must ensure that individual users are authenticated prior to authenticating via role or group authentication. This is to ensure that there is non-repudiation for actions taken.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35302; SV-46589

Comments:

CCI: CCI-000770The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.NIST SP 800-53 :: IA-2 (5) (b)NIST SP 800-53A :: IA-2 (5).2 (ii)NIST SP 800-53 Revision 4 :: IA-2 (5)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide security extensions to extend the SOAP protocol and provide secure authentication when accessing sensitive data.
STIG ID: SRG-APP-000156 **Rule ID:** SV-204749r508029_rule **Vul ID:** V-204749
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server provides extensions to the SOAP protocol that provide secure authentication. These protocols include, but are not limited to, WS_Security suite. Review policy and data owner protection requirements in order to identify sensitive data.

If secure authentication protocols are not utilized to protect data identified by data owner as requiring protection, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch does not offer a web services capability, and it does not support SOAP/WSDL web services. Therefore, the control does not apply to Elasticsearch.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers may provide a web services capability that could be leveraged to allow remote access to sensitive application data. A web service, which is a repeatable process used to make data available to remote clients, should not be confused with a web server.

Many web services utilize SOAP, which in turn utilizes XML and HTTP as a transport. Natively, SOAP does not provide security protections. As such, the application server must provide security extensions to enhance SOAP capabilities to ensure that secure authentication mechanisms are employed to protect sensitive data. The WS_Security suite is a widely used and acceptable SOAP security extension.

Legacy Ids: V-35304; SV-46591

Comments:

CCI: CCI-001941The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.NIST SP 800-53 Revision 4 :: IA-2 (8)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must disable identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.
STIG ID: SRG-APP-000163 **Rule ID:** SV-204750r508029_rule **Vul ID:** V-204750
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to ensure the application

server disables identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

If the application server is not configured to disable identifiers (individuals, groups, roles, and devices) after 35 days of inactivity, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider to disable identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Inactive identifiers pose a risk to systems and applications. Attackers that are able to exploit an inactive identifier can potentially obtain and maintain undetected access to the application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Applications need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Management of user identifiers is not applicable to shared information system accounts (e.g.,

guest and anonymous accounts). It is commonly the case that a user account is the name of an information system account associated with an individual.

To avoid having to build complex user management capabilities directly into their application, wise developers leverage the underlying OS or other user account management infrastructure (AD, LDAP) that is already in place within the organization and meets organizational user account management requirements.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35309; SV-46596

Comments:

CCI: CCI-000795The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.NIST SP 800-53 :: IA-4 eNIST SP 800-53A :: IA-4.1 (iii)NIST SP 800-53 Revision 4 :: IA-4 e

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must store only encrypted representations of passwords.
STIG ID: SRG-APP-000171 **Rule ID:** SV-204751r508029_rule **Vul ID:** V-204751
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server enforces the requirement to only store encrypted representations of passwords.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users and store only encrypted representations of passwords.

2. Additionally Password hashing settings references available for elasticsearch.yml configuration file.
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
Password hashing settings
xpack.security.authc.password_hashing.algorithm
(Static) Specifies the hashing algorithm that is used for secure user credential storage. See Table 2, “Password hashing algorithms”. Defaults to bcrypt.

3. Elasticsearch local users (native/file realm) passwords are stored salted/hashed.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html
l. Realms: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Applications must enforce password encryption when storing passwords.

Passwords need to be protected at all times and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read and easily compromised.

Application servers provide either a local user store or they integrate with enterprise user stores like LDAP. When the application server is responsible for creating or storing passwords, the application server must enforce the storage of encrypted representations of passwords.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35317; SV-46604

Comments:

CCI: CCI-000196The information system for password-based authentication stores only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must transmit only encrypted representations of passwords.
STIG ID: SRG-APP-000172 **Rule ID:** SV-204752r508029_rule **Vul ID:** V-204752
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server enforces the requirement to encrypt passwords when they are transmitted.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely

identify and authenticate users. When using an IdP, Elasticsearch does not transmit user account passwords.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Encrypting communications in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
k. Encrypting communications between Elasticsearch and LDAP:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-ldap
l. Generating Node Certificates:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#node-certificates
m. Encrypting communications between nodes in a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-transport
n. Encrypting HTTP client communications:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-http
o. Monitoring and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-monitoring.html
p. Configuring security in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/using-kibana-with-security.html
q. Configuring security in Logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Configure Filebeat to use security features:
https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Java Client and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/java-clients.html
t. Elasticsearch for Apache Hadoop Security:
https://www.elastic.co/guide/en/elasticsearch/hadoop/8.0/security.html

u. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords during transmission. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Application servers have the capability to utilize either certificates (tokens) or user IDs and passwords in order to authenticate. When the application server transmits or receives passwords, the passwords must be encrypted.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35318; SV-46605

Comments:

CCI: CCI-000197The information system for password-based authentication transmits only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must utilize encryption when using LDAP for authentication.
STIG ID: SRG-APP-000172 **Rule ID:** SV-204753r508029_rule **Vul ID:** V-204753
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application

server enforces the requirement to encrypt LDAP traffic.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

When using LDAP for authentication, configure the application server to encrypt LDAP traffic.

1. Encrypt communications between Elasticsearch and LDAP. For more information, see https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html#tls-ldap

2. Configure the realm's TLS settings on each node to trust certificates signed by the CA that signed your LDAP server certificates. The following example demonstrates how to trust a CA certificate, cacert.pem, located within the Elasticsearch configuration directory (ES_PATH_CONF):

xpack:
security:
authc:
realms:
ldap:
ldap1:
order: 0
url: "ldaps://ldap.example.com:636"
ssl:
certificate_authorities: ["ES_PATH_CONF/cacert.pem"]

The CA certificate must be a PEM encoded.
You can also specify the individual server certificates rather than the CA certificate, but this is only recommended if you have a single LDAP server or the certificates are self-signed.

3. Set the url attribute in the realm configuration to specify the LDAPS protocol and the secure port number. For example, url: ldaps://ldap.example.com:636.

4. Restart Elasticsearch.

Note: By default, when you configure Elasticsearch to connect to an LDAP server using SSL/TLS, it attempts to verify the hostname or IP address specified with the url attribute in the realm configuration with the values in the certificate. If the values in the certificate and realm configuration do not match, Elasticsearch does not allow a connection to the LDAP server. This is done to protect against man-in-the-middle attacks. If necessary, you can disable this behavior by setting the ssl.verification_mode property to certificate.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Encrypting communications in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
k. Encrypting communications between Elasticsearch and LDAP:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html#tls-ldap
l. Generating Node Certificates:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#node-certificates
m. Encrypting communications between nodes in a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-transport
n. Encrypting HTTP client communications:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-http
o. Monitoring and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-monitoring.html
p. Configuring security in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/using-kibana-with-security.html
q. Configuring security in Logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Configure Filebeat to use security features:
https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Java Client and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/java-clients.html
t. Elasticsearch for Apache Hadoop Security:
https://www.elastic.co/guide/en/elasticsearch/hadoop/8.0/security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords during transmission.

Application servers have the capability to utilize LDAP directories for authentication. If LDAP connections are not protected during transmission, sensitive authentication credentials can be stolen. When the application server utilizes LDAP, the LDAP traffic must be encrypted.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35319; SV-46606

Comments:

CCI: CCI-000197The information system for password-based authentication transmits only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must perform RFC 5280-compliant certification path validation.
STIG ID: SRG-APP-000175 **Rule ID:** SV-204754r508029_rule **Vul ID:** V-204754
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine whether the application server provides PKI functionality that validates certification paths in accordance with RFC 5280.

If PKI is not being used, this is NA.

If the application server is using PKI, but it does not perform this requirement, this is a

finding.

Fix Text:
Step/Recommendation:

1. At this time, the Elastic Stack does not support RFC-5280. However, an enhancement request has been submit to add this capability to the Elastic Stack.

Reference:

a. Internal support for this is tracked in enhancement requests :
https://github.com/elastic/enhancements/issues?q=is%3Aissue+is%3Aopen+CRL+

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A certificate's certification path is the path from the end entity certificate to a trusted root certification authority (CA). Certification path validation is necessary for a relying party to make an informed decision regarding acceptance of an end entity certificate. Certification path validation includes checks such as certificate issuer trust, time validity and revocation status for each certificate in the certification path. Revocation status information for CA and subject certificates in a certification path is commonly provided via certificate revocation lists (CRLs) or online certificate status protocol (OCSP) responses.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35322; SV-46609

Comments:

CCI: CCI-000185The information system for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2) (a)

Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: Only authenticated system administrators or the designated PKI Sponsor for the application server must have access to the web servers private key.
STIG ID: SRG-APP-000176 **Rule ID:** SV-204755r508029_rule **Vul ID:** V-204755
Severity: CAT II

Documentable: No

Check Content:
Review application server configuration and documentation to ensure the application server enforces authorized access to the corresponding private key.

If the application server is not configured to enforce authorized access to the corresponding private key, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin

- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html

r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and can pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys. Java-based application servers utilize the Java keystore, which provides storage for cryptographic keys and certificates. The keystore is usually maintained in a file stored on the file system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35324; SV-46611

Comments:

CCI: CCI-000186The information system for PKI-based authentication enforces authorized access to the corresponding private key.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must map the authenticated identity to the individual user

or group account for PKI-based authentication.
STIG ID: SRG-APP-000177 **Rule ID:** SV-204756r508029_rule **Vul ID:** V-204756
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server provides a PKI integration capability that meets DoD PKI infrastructure requirements.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a

different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport

Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The cornerstone of PKI is the private key used to encrypt or digitally sign information. The key by itself is a cryptographic value that does not contain specific user information, but the key can be mapped to a user. Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Application servers must provide the capability to utilize and meet requirements of the DoD Enterprise PKI infrastructure for application authentication.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35325; SV-46612

Comments:

CCI: CCI-000187The information system for PKI-based authentication maps the authenticated identity to the account of the individual or group.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
STIG ID: SRG-APP-000178 **Rule ID:** SV-204757r508029_rule **Vul ID:** V-204757
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if any interfaces which are provided for authentication purposes display the user's password when it is typed into the data entry field.

If authentication information is not obfuscated when entered, this is a finding.

Fix Text:
Steps/Recommendation:

1. Kibana can be used as the front end, to prohibit the display of passwords in clear text on the command line.

2. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI). The recommendation is to integrate Elasticsearch with these services to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

References:

a. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. Rest APIs: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/rest-apis.html
c. Kibana Guide: https://www.elastic.co/guide/en/kibana/8.0/index.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To prevent the compromise of authentication information during the authentication process, the application server authentication screens must obfuscate input so an unauthorized user cannot view a password, PIN, or any other authenticator value as it is being typed.

This can occur when a user is authenticating to the application server through the web management interface or command line interface. The application server must obfuscate all passwords, PINs, or other authenticator information when typed. User ID is not required to be obfuscated.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35328; SV-46615

Comments:

CCI: CCI-000206The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.NIST SP 800-53 :: IA-6NIST SP 800-53A :: IA-6.1NIST SP 800-53 Revision 4 :: IA-6

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must utilize FIPS 140-2 approved encryption modules when authenticating users and processes.
STIG ID: SRG-APP-000179 **Rule ID:** SV-204758r508029_rule **Vul ID:** V-204758
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine which version of TLS is being used.

If the application server is not using TLS when authenticating users or non-FIPS-approved SSL versions are enabled, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Encryption is only as good as the encryption modules utilized. Unapproved cryptographic module algorithms cannot be verified and cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised due to weak algorithms. The use of TLS provides confidentiality of data in transit between the application server and client.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-35329; SV-46616

Comments:

CCI: CCI-000803The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance for such authentication.NIST SP 800-53 :: IA-7NIST SP 800-53A :: IA-7.1NIST SP 800-53 Revision 4 :: IA-7

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide a log reduction capability that supports on-demand reporting requirements.
STIG ID: SRG-APP-000181 **Rule ID:** SV-204759r508029_rule **Vul ID:** V-204759
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and server configuration to determine if the application server is configured to provide log reduction with on-demand reporting.

If the application server is not configured to provide log reduction with on-demand reporting, or is not configured to send its logs to a centralized log system, this is a finding.

Fix Text:
Steps/Recommendation:

1. You can use the Elasticsearch APIs to perform on-demand reporting.
curl -X GET "localhost:9200/my-index-000001/_search?pretty"

2. Recommend usage of Kibana UI and Beats dashboards for a more robust user experience.

References:

a. Search: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
b. Mapping -> Mapping Parameters -> fielddata:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fielddata.html
c. Index and Search Analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html
d. Kibana Query: https://www.elastic.co/guide/en/kibana/8.0/kuery-query.html
e. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html

f. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The ability to generate on-demand reports, including after the log data has been subjected to log reduction, greatly facilitates the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Log reduction is a process that manipulates collected log information and organizes such information in a summary format that is more meaningful to analysts. The report generation capability provided by the application must support on-demand (i.e., customizable, ad-hoc, and as needed) reports.

Instead of the application server providing the log reduction function; it is also accepted practice to configure the application server to send its logs to a centralized log system that can be used to provide the log reduction with reporting capability. Security Incident Event Management (SIEM) systems are an example of such a solution.

To fully understand and investigate an incident within the components of the application server, the application server, must be configured to provide log reduction and on-demand reporting or be configured to send its logs to a centralized log system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57527; SV-71803

Comments:

CCI: CCI-001876The information system provides an audit reduction capability that supports on-demand reporting requirements.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must identify prohibited mobile code.

STIG ID: SRG-APP-000206 **Rule ID:** SV-204760r508029_rule **Vul ID:** V-204760
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server is configured to identify prohibited mobile code.

If the application server is not configured to identify prohibited mobile code, this is a finding.

Fix Text:
Step/Recommendation:

1. For the Elastic-hosted Elasticsearch Service, per 800-53 (SC-18 Mobile Code), Elasticsearch service currently does not make use of mobile code and has set no usage restrictions of mobile code (e.g., JavaScript, VBScript, ActiveX, etc.) within the Elastic Cloud application, although protections are configured to identify anomalous activity. An end user's workstation should have endpoint protection and browser controls implemented to prevent the execution of unauthorized mobile code.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Mobile code is defined as software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

Mobile code technologies include: Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

Application servers must meet policy requirements regarding the deployment and/or use of mobile code. This includes digitally signing applets in order to provide a means for the client

to establish application authenticity and prohibit unauthorized code from being used.

Legacy Ids: V-57547; SV-71823

Comments:

CCI: CCI-001166The information system identifies organization-defined unacceptable mobile code.NIST SP 800-53 :: SC-18 (1)NIST SP 800-53A :: SC-18 (1).1 (i)NIST SP 800-53 Revision 4 :: SC-18 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must separate hosted application functionality from application server management functionality.
STIG ID: SRG-APP-000211 **Rule ID:** SV-204761r508029_rule **Vul ID:** V-204761
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to verify that the application server separates admin functionality from hosted application functionality.

If the application server does not separate application server admin functionality from hosted application functionality, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch natively does not provide a GUI interface. Recommended to use the Kibana UI for managing the Elastic Stack.

Access to individual features is governed by Elasticsearch and Kibana privileges.

2. The separation of user functionality from application server management can be accomplished by moving management functions to a separate IP address or port—a separate Kibana space for administrative functions and another separate space for end user-related functionality.

Each Elasticsearch node has two different network interfaces. Clients send requests to Elasticsearch’s REST APIs using its HTTP interface, but nodes communicate with other nodes using the transport interface. The transport interface is also used for communication with remote clusters.

Transport settings
The following settings can be configured for the internal transport that communicates over TCP. Some of the available settings are presented below for brevity.

transport.port
(Static) The port to bind for communication between nodes. Accepts a single value or a range. If a range is specified, the node will bind to the first available port in the range. Set this setting to a single port, not a range, on every master-eligible node.
Defaults to 9300-9400.

transport.publish_port
(Static) The port of the transport publish address. Set this parameter only if you need the publish port to be different from transport.port. Defaults to the port assigned via transport.port.

transport.bind_host
(Static) The network address(es) to which the node should bind in order to listen for incoming transport connections. Accepts a list of IP addresses, hostnames, and special values. Defaults to the address given by transport.host or network.bind_host. Use this setting only if you require to bind to multiple addresses or to use different addresses for publishing and binding, and you also require different binding configurations for the transport and HTTP interfaces.

transport.publish_host
(Static) The network address at which the node can be contacted by other nodes. Accepts an IP address, a hostname, or a special value. Defaults to the address given by transport.host or network.publish_host. Use this setting only if you require to bind to multiple addresses or to use different addresses for publishing and binding, and you also require different binding configurations for the transport and HTTP interfaces.

transport.host
(Static) Sets the address of this node for transport traffic. The node will bind to this address and will also use it as its transport publish address. Accepts an IP address, a hostname, or a special value. Use this setting only if you require different configurations for the transport and HTTP interfaces.

Defaults to the address given by network.host.

3. The separation of user functionality from application server management can be accomplished by creating separate Kibana spaces for administrative functions and another separate space for end user-related functionality.

Spaces can be managed via the Kibana interface through the main menu, Stack Management > Spaces. This view provides actions to create, edit, and delete spaces.

References:

a. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html
b. Networking:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-network.html
c. Kibana spaces: https://www.elastic.co/guide/en/kibana/master/xpack-spaces.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server consists of the management interface and hosted applications. By separating the management interface from hosted applications, the user must authenticate as a privileged user to the management interface before being presented with management functionality. This prevents non-privileged users from having visibility to functions not available to the user. By limiting visibility, a compromised non-privileged account does not offer information to the attacker to functionality and information needed to further the attack on the application server.

Application server management functionality includes functions necessary to administer the application server and requires privileged access via one of the accounts assigned to a management role. The hosted application and hosted application functionality consists of the assets needed for the application to function, such as the business logic, databases, user authentication, etc.

The separation of application server administration functionality from hosted application functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, network addresses, network ports, or combinations of these methods, as appropriate.

Legacy Ids: V-35376; SV-46663

Comments:

CCI: CCI-001082The information system separates user functionality (including user interface services) from information system management functionality.NIST SP 800-53 :: SC-2NIST SP 800-53A :: SC-2.1NIST SP 800-53 Revision 4 :: SC-2

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured to mutually authenticate connecting

proxies, application servers or gateways.
STIG ID: SRG-APP-000219 **Rule ID:** SV-204762r508029_rule **Vul ID:** V-204762
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation, system security plan and application data protection requirements.

If the connected web proxy is exposed to an untrusted network or if data protection requirements specified in the system security plan mandate the need to establish the identity of the connecting application server, proxy or application gateway and the application server is not configured to mutually authenticate the application server, proxy server or gateway, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports mutual TLS for the HTTP layer. A proxy should be placed in front of the cluster to satisfy this control, which can be configured for mTLS with Elasticsearch.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application architecture may sometimes require a configuration where an application server is placed behind a web proxy, an application gateway or communicates directly with another application server. In those instances, the application server hosting the service/application is considered the server. The application server, proxy or application gateway consuming the hosted service is considered a client. Authentication is accomplished

via the use of certificates and protocols such as TLS mutual authentication. Authentication must be performed when the proxy is exposed to an untrusted network or when data protection requirements specified in the system security plan mandate the need to establish the identity of the connecting application server, proxy or application gateway.

Connect clients to Elasticsearch:
When you start Elasticsearch for the first time, TLS is configured automatically for the HTTP layer. A CA certificate is generated and stored on disk at $ES_HOME/config/certs/http_ca.crt. The hex-encoded SHA-256 fingerprint of this certificate is also output to the terminal. Any clients that connect to Elasticsearch, such as the Elasticsearch Clients, Beats, standalone Elastic Agents, and Logstash must validate that they trust the certificate that Elasticsearch uses for HTTPS. Fleet Server and Fleet-managed Elastic Agents are automatically configured to trust the CA certificate. Other clients can establish trust by using either the fingerprint of the CA certificate or the CA certificate itself.

Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Legacy Ids: V-35381; SV-46668

Comments:

CCI: CCI-001184The information system protects the authenticity of communications sessions.NIST SP 800-53 :: SC-23NIST SP 800-53A :: SC-23.1NIST SP 800-53 Revision 4 :: SC-23

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must invalidate session identifiers upon user logout or other session termination.
STIG ID: SRG-APP-000220 **Rule ID:** SV-204763r508029_rule **Vul ID:** V-204763
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and organizational policy to determine if the system is configured to terminate administrator sessions upon administrator logout or any other organization- or policy-defined session termination events, such as idle time limit exceeded.

If the configuration is not set to terminate administrator sessions per defined events, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to invalidate session identifiers upon user logout or other session termination or any other organization- or policy-defined session termination events.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If communications sessions remain open for extended periods of time even when unused, there is the potential for an adversary to hijack the session and use it to gain access to the device or networks to which it is attached. Terminating sessions after a logout event or

after a certain period of inactivity is a method for mitigating the risk of this vulnerability. When a user management session becomes idle, or when a user logs out of the management interface, the application server must terminate the session.

Legacy Ids: V-35415; SV-46702

Comments:

CCI: CCI-001185The information system invalidates session identifiers upon user logout or other session termination.NIST SP 800-53 :: SC-23 (1)NIST SP 800-53A :: SC-23 (1).1NIST SP 800-53 Revision 4 :: SC-23 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate a unique session identifier for each session.
STIG ID: SRG-APP-000223 **Rule ID:** SV-204764r508029_rule **Vul ID:** V-204764
Severity: CAT II

Documentable: No

Check Content:
Review the application server session management configuration settings in either the application server management console, application server initialization or application server configuration files to determine if the application server is configured to generate a unique session identifier for each session.

If the application server is not configured to generate a unique session identifier for each session, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to generate a unique session identifier for each session.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html

b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Unique session IDs are the opposite of sequentially generated session IDs, which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of session identifiers. Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

Application servers must generate a unique session identifier for each application session so as to prevent session hijacking.

Legacy Ids: V-57549; SV-71825

Comments:

CCI: CCI-001664The information system recognizes only session identifiers that are system-generated.NIST SP 800-53 :: SC-23 (3)NIST SP 800-53A :: SC-23 (3).1 (ii)NIST SP 800-53 Revision 4 :: SC-23 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must recognize only system-generated session identifiers.
STIG ID: SRG-APP-000223 **Rule ID:** SV-204765r508029_rule **Vul ID:** V-204765
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server recognizes only system-generated session identifiers.

If the application server does not recognize only system-generated session identifiers, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to recognize only system-generated session identifiers.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This requirement focuses on communications protection at the application session, versus network packet level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted.

Unique session IDs are the opposite of sequentially generated session IDs which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of said identifiers.

Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

Legacy Ids: V-35421; SV-46708

Comments:

CCI: CCI-001664The information system recognizes only session identifiers that are system-generated.NIST SP 800-53 :: SC-23 (3)NIST SP 800-53A :: SC-23 (3).1 (ii)NIST SP 800-53 Revision 4 :: SC-23 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate a unique session identifier using a FIPS 140-2 approved random number generator.
STIG ID: SRG-APP-000224 **Rule ID:** SV-204766r508029_rule **Vul ID:** V-204766
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and documentation to determine if the application server uses a FIPS 140-2 approved random number generator to create unique session identifiers.

Have a user log onto the application server to determine if the session IDs generated are random and unique.

If the application server does not generate unique session identifiers and does not use a FIPS 140-2 random number generator to create the randomness of the session ID, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to generate a unique session identifier using a FIPS 140-2 approved random number generator.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server will use session IDs to communicate between modules or applications within the application server and between the application server and users. The session ID allows the application to track the communications along with credentials that may have been used to authenticate users or modules.

Unique session IDs are the opposite of sequentially generated session IDs which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of said identifiers.

Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

Legacy Ids: V-35422; SV-46709

Comments:

CCI: CCI-001188The information system generates unique session identifiers for each session with organization-defined randomness requirements.NIST SP 800-53 :: SC-23 (4)NIST SP 800-53A :: SC-23 (4).1 (ii)NIST SP 800-53 Revision 4 :: SC-23 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured to perform complete application deployments.
STIG ID: SRG-APP-000225 **Rule ID:** SV-204767r508029_rule **Vul ID:** V-204767
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and documentation to ensure the system is configured to perform complete application deployments.

If the application server is not configured to ensure complete application deployments or

provides no rollback functionality, this is a finding.

Fix Text:
Steps/Recommendation:

1. As part of the hosted Elasticsearch Service offering, customers may configure how they wish to run backups to enable rollback or restore of their configurations. Elastic is responsible for SaaS and system wide capabilities for snapshot and restore operations at the SaaS layer level. Use of ECE, ECK, or Elastic Cloud is recommended; rollback or prevention of deployment if errors are encountered is not supported by Elastic for "self-managed" implementations.

ECE supports rolling upgrades on an Elasticsearch cluster to be upgraded one node at a time so upgrading does not interrupt service.

Note: When upgrading to Elasticsearch 8.0 and later, you must first upgrade to 7.17 whether you opt to perform a rolling upgrade (upgrade one node at a time) or a full-cluster restart upgrade.

Before you start to upgrade your cluster you should do the following.
- Check the deprecation log to see if you are using any deprecated features and update your code accordingly.
- Review the breaking changes and make any necessary changes to your code and configuration for version.
- If you use any plugins, make sure there is a version of each plugin that is compatible with Elasticsearch version.
- Test the upgrade in an isolated environment before upgrading your production cluster.
- Back up your data by taking a snapshot!

2. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to enable rollback or restore to the last known good configuration in the event of errors that occur during application deployment and to prevent deployment if errors are encountered.

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Rolling upgrades:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/rolling-upgrades.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the

Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system.

When an application is deployed to the application server, if the deployment process does not complete properly and without errors, there is the potential that some application files may not be deployed or may be corrupted and an application error may occur during runtime.

The application server must be able to perform complete application deployments. A partial deployment can leave the server in an inconsistent state. Application servers may provide a transaction rollback function to address this issue.

Legacy Ids: V-35423; SV-46710

Comments:

CCI: CCI-001190The information system fails to an organization-defined known-state for organization-defined types of failures.NIST SP 800-53 :: SC-24NIST SP 800-53A :: SC-24.1 (iv)NIST SP 800-53 Revision 4 :: SC-24

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide a clustering capability.
STIG ID: SRG-APP-000225 **Rule ID:** SV-204768r508029_rule **Vul ID:** V-204768
Severity: CAT II

Documentable: No

Check Content:
This requirement is dependent upon system MAC and confidentiality.

If the system MAC and confidentiality levels do not specify redundancy requirements, this requirement is NA.

Review the application server configuration and documentation to ensure the application server is configured to provide clustering functionality.

If the application server is not configured to provide clustering or some form of failover functionality, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch provides a clustering capability by design.
A single instance of Elasticsearch is a node. A collection of connected nodes is called a cluster.

Nodes are added to a cluster to increase its capacity and reliability. By default, a node is both a data node and eligible to be elected as the master node that controls the cluster. A node can be configured for a specific purpose, such as handling ingest requests.

By default, a node is all of the following types: master-eligible, data, ingest, and (if available) machine learning. All data nodes are also transform nodes.

As the cluster grows and in particular if you have large machine learning jobs or continuous transforms, consider separating dedicated master-eligible nodes from dedicated data nodes, machine learning nodes, and transform nodes.

Node roles can be defined by setting node.roles. If this is not set, then the node has the following roles by default:

master
data
data_content
data_hot
data_warm
data_cold
data_frozen
ingest
ml
remote_cluster_client
transform

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This requirement is dependent upon system MAC and confidentiality. If the system MAC and confidentiality levels do not specify redundancy requirements, this requirement is NA.

Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. When application failure is encountered, preserving application state facilitates application restart and return to the operational mode of the organization with less disruption of mission/business processes.

Clustering of multiple application servers is a common approach to providing fail-safe application availability when system MAC and confidentiality levels require redundancy.

Legacy Ids: V-35424; SV-46711

Comments:

CCI: CCI-001190The information system fails to an organization-defined known-state for organization-defined types of failures.NIST SP 800-53 :: SC-24NIST SP 800-53A :: SC-24.1 (iv)NIST SP 800-53 Revision 4 :: SC-24

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.
STIG ID: SRG-APP-000225 **Rule ID:** SV-204769r508029_rule **Vul ID:** V-204769
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server fails to a secure state if system initialization fails, shutdown fails, or aborts fail.

If the application server cannot be configured to fail securely, this is a finding.

Fix Text:
Steps/Recommendation:

Elasticsearch does not currently offer to fail to a secure state if system initialization fails, shutdown fails, or aborts fail; in that the way to shut down a node is to terminate the process.

Recommend configuring Elasticsearch for high availability. The system will fail over to the backup capability as part of the customer contingency plan, in which case, the system doesn't "fail" and the customer can investigate the primary component's status without interruption of service.

1. Elasticsearch provides a clustering capability by design and can be configured in a high-availability (HA) cluster. Elasticsearch offers a number of features to achieve HA despite failures.

- With proper planning, a cluster can be designed for resilience to many of the things that commonly go wrong, from the loss of a single node or network connection right up to a zone-wide outage such as power loss.
- Use cross-cluster replication to replicate data to a remote follower cluster which may be in a different data centre or even on a different continent from the leader cluster. The follower cluster acts as a hot standby, ready fail over in the event of a disaster so severe that the leader cluster fails. The follower cluster can also act as a geo-replica to serve searches from nearby clients.
- The last line of defense against data loss is to take regular snapshots of the cluster so that it can be restored elsewhere if needed.

Designing for resilience
A resilient cluster requires redundancy for every required cluster component. This means a resilient cluster must have:
- At least three master-eligible nodes
- At least two nodes of each role
- At least two copies of each shard (one primary and one or more replicas)

Back up a cluster
To have a complete backup for a cluster:
- Back up the data
- Back up the cluster configuration
- Back up the security configuration

2. If using Elasticsearch as a SaaS product (Elastic-hosted), recommend a minimum of three availability zones to enable Elastic Cloud Enterprise to create clusters with a tiebreaker.

High availability
- Fault tolerance for Elastic Cloud Enterprise is based around the concept of availability zones.
- An availability zone contains resources available to an Elastic Cloud Enterprise installation that are isolated from other availability zones to safeguard against potential failure.
- If there are only two availability zones in total in an installation, no tiebreaker is created.

3. Refer to the cloud provider options of Regions and Availability Zones for high-availability (HA) cluster for hosting the Elastic cluster.

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html
c. Set up a cluster for high availability:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability.html
d. Designing for resilience:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability-cluster-design.html
e. Cross-cluster replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html
f. Create a snapshot:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/snapshots-take-snapshot.html
g. High availability: https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-ha.html
h. Bootstrap Checks:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/bootstrap-checks.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Fail-secure is a condition achieved by the application server in order to ensure that in the event of an operational failure, the system does not enter into an unsecure state where intended security properties no longer hold. Preserving information system state information also facilitates system restart and return to the operational mode of the organization with less disruption of mission-essential processes.

Legacy Ids: V-57553; SV-71829

Comments:

CCI: CCI-001190The information system fails to an organization-defined known-state for organization-defined types of failures.NIST SP 800-53 :: SC-24NIST SP 800-53A :: SC-24.1 (iv)NIST SP 800-53 Revision 4 :: SC-24

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect the confidentiality and integrity of all information at rest.

STIG ID: SRG-APP-000231 **Rule ID:** SV-204770r508029_rule **Vul ID:** V-204770
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to ensure the application server is protecting the confidentiality and integrity of all information at rest.

If the confidentiality and integrity of all information at rest is not protected, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When data is written to digital media such as hard drives, mobile computers, external/removable hard drives, personal digital assistants, flash/thumb drives, etc., there is risk of data loss and data compromise.

Fewer protection measures are needed for media containing information determined by the

organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed the physical access controls where the media resides provide adequate protection.

As part of a defense-in-depth strategy, data owners and DoD consider routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information.

The strength of mechanisms is commensurate with the classification and sensitivity of the information.

The application server must directly provide, or provide access to, cryptographic libraries and functionality that allow applications to encrypt data when it is stored.

Legacy Ids: V-57555; SV-71831

Comments:

CCI: CCI-001199The information system protects the confidentiality and/or integrity of organization-defined information at rest.NIST SP 800-53 :: SC-28NIST SP 800-53A :: SC-28.1NIST SP 800-53 Revision 4 :: SC-28

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must employ cryptographic mechanisms to ensure confidentiality and integrity of all information at rest when stored off-line.
STIG ID: SRG-APP-000231 **Rule ID:** SV-204771r508029_rule **Vul ID:** V-204771
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to ensure the system is protecting the confidentiality and integrity of all application server data at rest when stored off-line.

If the application server is not configured to protect all application server data at rest when stored off-line, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.

Application servers generate information throughout the course of their use, most notably, log data. If the data is not encrypted while at rest, the data used later for forensic investigation cannot be guaranteed to be unchanged and cannot be used for prosecution of an attacker. To accomplish a credible investigation and prosecution, the data integrity and information confidentiality must be guaranteed.

Application servers must provide the capability to protect all data, especially log data, so as to ensure confidentiality and integrity.

Legacy Ids: V-35426; SV-46713

Comments:

CCI: CCI-001199The information system protects the confidentiality and/or integrity of

organization-defined information at rest.NIST SP 800-53 :: SC-28NIST SP 800-53A :: SC-28.1NIST SP 800-53 Revision 4 :: SC-28

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must check the validity of all data inputs to the management interface, except those specifically identified by the organization.
STIG ID: SRG-APP-000251 **Rule ID:** SV-204772r508029_rule **Vul ID:** V-204772
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the system checks the validity of information inputs to the management interface, except those specifically identified by the organization.

If the management interface data inputs are not validated, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommended using the Kibana UI to manage the Elastic Stack and that Kibana performs input validation checks. Access to individual features is governed by Elasticsearch and Kibana privileges.

References:

a. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html
b. Security best practices:
https://www.elastic.co/guide/en/kibana/8.0/security-best-practices.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Invalid user input occurs when a user inserts data or characters into an applications data entry field and the application is unprepared to process that data. This results

in unanticipated application behavior potentially leading to an application or information system compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

Application servers must ensure their management interfaces perform data input validation checks. Input validation consists of evaluating user input and ensuring that only allowed characters are utilized. An example is ensuring that the interfaces are not susceptible to SQL injection attacks.

Legacy Ids: V-35436; SV-46723

Comments:

CCI: CCI-001310The information system checks the validity of organization-defined inputs.NIST SP 800-53 :: SI-10NIST SP 800-53A :: SI-10.1NIST SP 800-53 Revision 4 :: SI-10

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must identify potentially security-relevant error conditions.
STIG ID: SRG-APP-000266 **Rule ID:** SV-204773r508029_rule **Vul ID:** V-204773
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the system identifies potentially security-relevant error conditions on the server.

If this function is not performed, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to generate log records for potentially security-relevant error conditions like when successful/unsuccessful attempts to modify privileges occur.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see

https://www.elastic.co/subscriptions.

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to generate log records for potentially security-relevant error conditions like when successful/unsuccessful attempts to modify privileges occur.

4. Recommend establishing an alert to appropriate personnel for potentially security-relevant error conditions.

The Elastic Stack API can be used to setup alerts. However, it is recommended to use the Kibana UI for a better user experience.

5. Watcher
The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. They can be tailor to meet specific needs.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
e. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/how-monitoring-works.html
f. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
g. Kibana Alerts: https://www.elastic.co/guide/en/kibana/8.0/kibana-alerts.html
h. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html

i. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
j. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
k. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
l. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
m. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
n. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
o. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
p. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
q. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
r. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
s. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
t. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The structure and content of error messages need to be carefully considered by the organization and development team. Any application providing too much information in error logs and in administrative messages to the screen risks compromising the data and security of the application and system. The extent to which the application server is able to identify and handle error conditions is guided by organizational policy and operational requirements. Adequate logging levels and system performance capabilities need to be balanced with data protection requirements.

The structure and content of error messages needs to be carefully considered by the organization and development team.

Application servers must have the capability to log at various levels which can provide log entries for potential security-related error events.

An example is the capability for the application server to assign a criticality level to a failed logon attempt error message, a security-related error message being of a higher criticality.

Legacy Ids: V-57567; SV-71843

Comments:

CCI: CCI-001312The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.NIST SP 800-53 :: SI-11 bNIST SP 800-53A :: SI-11.1 (iii)NIST SP 800-53 Revision 4 :: SI-11 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must only generate error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages.
STIG ID: SRG-APP-000266 **Rule ID:** SV-204774r508029_rule **Vul ID:** V-204774
Severity: CAT II

Documentable: No

Check Content:
Review system documentation and logs to determine if the application server writes sensitive information such as passwords or private keys into the logs and administrative messages.

If the application server writes sensitive or potentially harmful information into the logs and administrative messages, this is a finding.

Fix Text:
Steps/Recommendation:

1. End users will typically see very generic error messages designed to be brief and high level. The default logging level of Elasticsearch and Kibana adheres to the control.

2. Configure any custom application code not to divulge sensitive information or information useful for system identification in the error information.

References:

a. Logging: https://www.elastic.co/guide/en/elasticsearch/reference/current/logging.html
b. Kibana reporting troubleshooting:

https://www.elastic.co/guide/en/kibana/8.0/reporting-troubleshooting.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Any application providing too much information in error logs and in administrative messages to the screen risks compromising the data and security of the application and system. The structure and content of error messages needs to be carefully considered by the organization and development team.

The application server must not log sensitive information such as passwords, private keys, or other sensitive data. This requirement pertains to logs that are generated by the application server and application server processes, not the applications that may reside on the application server. Those errors are out of the scope of these requirements.

Legacy Ids: V-35440; SV-46727

Comments:

CCI: CCI-001312The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.NIST SP 800-53 :: SI-11 bNIST SP 800-53A :: SI-11.1 (iii)NIST SP 800-53 Revision 4 :: SI-11 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must restrict error messages only to authorized users.
STIG ID: SRG-APP-000267 **Rule ID:** SV-204775r508029_rule **Vul ID:** V-204775
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and documentation to determine if the application server will restrict access to error messages so only authorized users may view or otherwise access them.

If the application server cannot be configured to restrict access to error messages to only

authorized users, this is a finding.

Fix Text:
Steps/Recommendation:

1. End users will typically see very generic error messages designed to be brief and high level. The default logging level of Elasticsearch and Kibana adheres to the control.

Configure any custom application code not to divulge sensitive information or information useful for system identification in the error information.

2. Enabling security protects Elasticsearch clusters by preventing unauthorized access with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

References:

a. Logging: https://www.elastic.co/guide/en/elasticsearch/reference/current/logging.html
b. Kibana reporting troubleshooting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-troubleshooting.html
c. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html
d. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the application provides too much information in error logs and administrative messages to the screen, this could lead to compromise. The structure and content of error messages need to be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Application servers must protect the error messages that are created by the application server. All application server users' accounts are used for the management of the server and the applications residing on the application server. All accounts are assigned to a certain role with

corresponding access rights. The application server must restrict access to error messages so only authorized users may view them. Error messages are usually written to logs contained on the file system. The application server will usually create new log files as needed and must take steps to ensure that the proper file permissions are utilized when the log files are created.

Legacy Ids: V-35441; SV-46728

Comments:

CCI: CCI-001314The information system reveals error messages only to organization-defined personnel or roles.NIST SP 800-53 :: SI-11 cNIST SP 800-53A :: SI-11.1 (iv)NIST SP 800-53 Revision 4 :: SI-11 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use cryptographic mechanisms to protect the integrity of log tools.
STIG ID: SRG-APP-000290 **Rule ID:** SV-204776r508029_rule **Vul ID:** V-204776
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server log tools have been cryptographically signed to protect the integrity of the tools.

If the application server log tools have not been cryptographically signed, this is a finding.

Fix Text:
Steps/Recommendation:

Currently, Elastic does not sign any of the jars/code in Elasticsearch.

1. For the Elastic cloud hosted service offerings, Elastic uses Auditbeat and Elastic Endpoint Security as host-based intrusion detection system and File Integrity Management (HIDS)/(FIM) on all hosts, specifying files and directories to be monitored for changes. File changes are detected in near real time and sent to Elasticsearch clusters in the Security Control Plane with metadata and cryptographic hashes of the file to enable further analysis. If unauthorized changes or anomalous connections are detected in the AWS infrastructure, an alert is generated from the Elasticsearch clusters to notify the Information Security team of an anomalous event.

2. For an on-premise Elasticsearch deployment, it is recommended that a third party

HIDS/FIM be implemented as a risk reduction method for this control.

3. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes. For example, the Elasticsearch directory contents include among others:
LICENSE.txt, NOTICE.txt, README.asciidoc, bin, config, data, jdk, lib, logs, modules, plugins

References:

a. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
b. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting the integrity of the tools used for logging purposes is a critical step in ensuring the integrity of log data. Log data includes all information (e.g., log records, log settings, and log reports) needed to successfully log information system activity.

It is not uncommon for attackers to replace the log tools or inject code into the existing tools for the purpose of providing the capability to hide or erase system activity from the logs.

To address this risk, log tools must be cryptographically signed in order to provide the capability to identify when the log tools have been modified, manipulated or replaced. An example is a checksum hash of the file or files.

Application server log tools must use cryptographic mechanisms to protect the integrity of the tools or allow cryptographic protection mechanisms to be applied to their tools.

Legacy Ids: V-35445; SV-46732

Comments:

CCI: CCI-001496The information system implements cryptographic mechanisms to protect the integrity of audit tools.NIST SP 800-53 :: AU-9 (3)NIST SP 800-53A :: AU-9 (3).1NIST SP 800-53 Revision 4 :: AU-9 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must automatically terminate a user session after organization-defined conditions or trigger events requiring a session disconnect.
STIG ID: SRG-APP-000295 **Rule ID:** SV-204777r508029_rule **Vul ID:** V-204777
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server is configured to close user sessions after defined conditions or trigger events are met.

If the application server is not configured or cannot be configured to disconnect users after defined conditions and trigger events are met, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to support automatically disconnect a user session after organization-defined conditions or trigger events requiring session disconnect.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout

Sets the session duration. By default, sessions stay active until the browser is closed. When this is set to an explicit idle timeout, closing the browser still requires the user to log back into Kibana.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g., 70ms, 5s, 3d, 1Y).

xpack.security.session.lifespan

Sets the maximum duration, also known as "absolute timeout". By default, a session can be renewed indefinitely. When this value is set, a session will end once its lifespan is exceeded,

even if the user is not idle. NOTE: if idleTimeout is not set, this setting will still cause sessions to expire.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
m. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: An attacker can take advantage of user sessions that are left open, thus bypassing the user authentication process.

To thwart the vulnerability of open and unused user sessions, the application server must be configured to close the sessions when a configured condition or trigger event is met.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

Legacy Ids: V-57401; SV-71673

Comments:

CCI: CCI-002361The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.NIST SP 800-53 Revision 4 :: AC-12

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server management interface must provide a logout capability for user-initiated communication session.
STIG ID: SRG-APP-000296 **Rule ID:** SV-204778r508029_rule **Vul ID:** V-204778
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server management interface provides a logout capability.

If the application server management interface does not provide a logout capability, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to

uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to provide a logout capability for user-initiated communication session.

2. Kibana logout and authentication settings are available at:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
Examples:
Local and global logout

During logout, both the Kibana session and Elasticsearch access/refresh token pair are invalidated. This is known as "local" logout.

Kibana can also initiate a "global" logout or Single Logout if it's supported by the external authentication provider and not explicitly disabled by Elasticsearch. In this case, the user is redirected to the external authentication provider for log out of all applications associated with the active provider session.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: If a user cannot explicitly end an application server management interface session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session.

The attacker will then have access to the application server management functions without going through the user authentication process.

To prevent this type of attack, the application server management interface must close user sessions when defined events are met and provide a logout function for users to explicitly close the session and free resources that were in use by the user.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57403; SV-71675

Comments:

CCI: CCI-002363The information system provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to organization-defined information resources.NIST SP 800-53 Revision 4 :: AC-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server management interface must display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.
STIG ID: SRG-APP-000297 **Rule ID:** SV-204779r508029_rule **Vul ID:** V-204779
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server management interface displays a logout message.

If the application server management interface does not display a logout message, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. Kibana as the front end can be used, and Kibana will display a logout message - the feature is not configurable. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to display an explicit logout message to users indicating the reliable termination of authenticated sessions.

2. Kibana logout and authentication settings are available at:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html

Examples:
Local logout: During logout, both the Kibana session and Elasticsearch access/refresh token pair are invalidated. This is known as "local" logout.

Global logout: Kibana can also initiate a "global" logout or Single Logout if it’s supported by the external authentication provider and not explicitly disabled by Elasticsearch. In this case, the user is redirected to the external authentication provider for log out of all applications associated with the active provider session.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Providing a logout capability to the user allows the user to explicitly close a session and free those resources used during the session.

If a user cannot explicitly end an application session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session.

The attacker will then have access to the application server management functions without going through the user authentication process.

To inform the user that the session has been reliably closed, a logout message must be displayed to the user.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57405; SV-71677

Comments:

CCI: CCI-002364The information system displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.NIST SP 800-53 Revision 4 :: AC-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.
STIG ID: SRG-APP-000313 **Rule ID:** SV-204780r508029_rule **Vul ID:** V-204780
Severity: CAT II

Documentable: No

Check Content:

Review the application server documentation to determine if the application associates organization-defined types of security attributes with organization-defined security attribute values to information in process.

If the application server does not associate the security attributes to information in process or the feature is not implemented, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a particular format.

3. Logstash and or Beats should be configured to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

4. All applications logs/events should associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

5. Recommend using Elasticsearch index templates where possible.

6. In Elasticsearch, mapping is the description of how documents and the fields they contain are stored and indexed. In the mapping, define the following, for example:
- The structure of the document (fields and data type of those fields)
- How to transform values before indexing
- What fields use for full-text searching

7. Update the index mapping definitions as needed to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

References:

a. Mapping: https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping.html
b. Index Template:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-templates.html
c. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
d. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
e. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
f. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
g. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html

h. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
i. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
j. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
k. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
l. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
m. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
n. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
o. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
p. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
q. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server provides a framework for applications to communicate between each other to form an overall well-designed application to perform a task. As the information traverses the application server and the components, the security attributes must be maintained. Without the association of security attributes to information, there is no basis for the application server or hosted applications to make security-related access control decisions. The security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information.

One example includes marking data as classified or FOUO. These security attributes may be assigned manually or during data processing, but either way, it is imperative these assignments are maintained while the data is in process. If the security attributes are lost when the data is being processed, there is the risk of a data compromise.

Legacy Ids: V-57407; SV-71679

Comments:

CCI: CCI-002263The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with

information in process.NIST SP 800-53 Revision 4 :: AC-16 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.
STIG ID: SRG-APP-000314 **Rule ID:** SV-204781r508029_rule **Vul ID:** V-204781
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation to determine if the application associates organization-defined types of security attributes with organization-defined security attribute values to information in transmission.

If the application server does not associate the security attributes to information in transmission or the feature is not implemented, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a particular format.

3. Logstash and/or Beats should be configured to associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.

4. All applications logs/events should associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.

5. Recommend using Elasticsearch index templates where possible.

6. In Elasticsearch, mapping is the description of how documents and the fields they contain are stored and indexed. In the mapping, you can define, for example, the following:
- The structure of the document (fields and data type of those fields)
- How to transform values before indexing

- What fields use for full-text searching

7. Update the index mapping definitions as needed to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

References:

a. Mapping: https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping.html
b. Index Template:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-templates.html
c. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
d. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
e. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
f. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
g. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
h. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
i. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
j. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
k. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
l. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
m. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
n. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
o. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
p. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
q. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server provides a framework for applications to communicate between each other to form an overall well-designed application to perform a task. As the information is transmitted, the security attributes must be maintained. Without the association

of security attributes to information, there is no basis for the application to make security-related access control decisions.

Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information.

One example includes marking data as classified or FOUO. These security attributes may be assigned manually or during data processing, but either way, it is imperative these assignments are maintained while the data is in transmission. If the security attributes are lost when the data is being transmitted, there is the risk of a data compromise.

Legacy Ids: V-57409; SV-71681

Comments:

CCI: CCI-002264The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.NIST SP 800-53 Revision 4 :: AC-16 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must control remote access methods.
STIG ID: SRG-APP-000315 **Rule ID:** SV-204782r508029_rule **Vul ID:** V-204782
Severity: CAT II

Documentable: No

Check Content:
Review organization policy, application server product documentation and configuration to determine if the system enforces the organization's requirements for remote connections.

If the system is not configured to enforce these requirements, or the remote connection settings are not in accordance with the requirements, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports mutual TLS for the HTTP layer. A proxy should be placed in front of the cluster to satisfy this control, which can be configured for mTLS with Elasticsearch to facilitate monitoring and control of web based or command line based administrative connections.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers provide remote access capability and must be able to enforce remote access policy requirements or work in conjunction with enterprise tools designed to enforce policy requirements. Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by logging connection activities of remote users.

Examples of policy requirements include, but are not limited to, authorizing remote access to the information system, limiting access based on authentication credentials, and monitoring for unauthorized access.

Legacy Ids: V-57413; SV-71685

Comments:

CCI: CCI-002314The information system controls remote access methods.NIST SP 800-53 Revision 4 :: AC-17 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide the capability to immediately disconnect or disable remote access to the management interface.
STIG ID: SRG-APP-000316 **Rule ID:** SV-204783r508029_rule **Vul ID:** V-204783
Severity: CAT II

Documentable: No

Check Content:

Review the application server product documentation and server configuration to ensure that there is a capability to immediately disconnect or disable remote access to the management interface.

If there is no capability, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to immediately disconnect or disable remote access to the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without the ability to immediately disconnect or disable remote access, an attack or other compromise taking progress would not be immediately stopped.

The application server must have the capability to immediately disconnect current users remotely accessing the management interface and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57415; SV-71687

Comments:

CCI: CCI-002322The organization provides the capability to expeditiously disconnect or disable remote access to the information system within the organization-defined time period.NIST SP 800-53 Revision 4 :: AC-17 (9)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
STIG ID: SRG-APP-000340 **Rule ID:** SV-204784r508029_rule **Vul ID:** V-204784
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to verify that non-privileged users cannot access or execute privileged functions.

Have a user logon as a non-privileged user and attempt to execute privileged functions.

If the user is capable of executing privileged functions, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm.

2. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

3. Configure the Application Server to allow only the ISSM (or individuals or roles appointed by the ISSM) to the required privileges.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
i. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
j. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Preventing non-privileged users from executing privileged functions mitigates

the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Restricting non-privileged users also prevents an attacker, who has gained access to a non-privileged account, from elevating privileges, creating accounts, and performing system checks and maintenance.

Legacy Ids: V-57399; SV-71671

Comments:

CCI: CCI-002235The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards/countermeasures.NIST SP 800-53 Revision 4 :: AC-6 (10)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide access logging that ensures users who are granted a privileged role (or roles) have their privileged activity logged.
STIG ID: SRG-APP-000343 **Rule ID:** SV-204785r508029_rule **Vul ID:** V-204785
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and log configuration to verify the application server logs privileged activity.

If the application server is not configured to log privileged activity, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

Note: If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log privileged activity.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/current/authorization.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
k. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
l. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
m. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: In order to be able to provide a forensic history of activity, the application server must ensure users who are granted a privileged role or those who utilize a separate distinct account when accessing privileged functions or data have their actions logged.

If privileged activity is not logged, no forensic logs can be used to establish accountability for privileged actions that occur on the system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57397; SV-71669

Comments:

CCI: CCI-002234The information system audits the execution of privileged functions.NIST SP 800-53 Revision 4 :: AC-6 (9)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide centralized management and configuration of the content to be captured in log records generated by all application components.
STIG ID: SRG-APP-000356 **Rule ID:** SV-204787r508029_rule **Vul ID:** V-204787
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server is part of a cluster.

If the application server is not part of a cluster, this requirement is NA.

If the application server is part of a cluster, verify that the log settings are managed and configured from a centralized management server.

If the log settings are not centrally managed, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch provides a clustering capability by design.

A single instance of Elasticsearch is a node. A collection of connected nodes is called a cluster.

Nodes are added to a cluster to increase its capacity and reliability. By default, a node is both a data node and eligible to be elected as the master node that controls the cluster. A node can be configured for a specific purpose, such as handling ingest requests.

2. Elasticsearch natively does not provide a GUI interface. Recommended to use the Kibana UI for centralized management and configuration of the content to be captured in log records generated by all application components.

Access to individual features is governed by Elasticsearch and Kibana privileges.

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html
c. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A clustered application server is made up of several servers working together to provide the user a failover and increased computing capability. To facilitate uniform logging in the event of an incident and later forensic investigation, the record format and logable events need to be uniform. This can be managed best from a centralized server.

Without the ability to centrally manage the content captured in the log records, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

Legacy Ids: V-57419; SV-71691

Comments:

CCI: CCI-001844The information system provides centralized management and configuration of the content to be captured in audit records generated by organization-defined information system components.NIST SP 800-53 Revision 4 :: AU-3 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must limit the number of concurrent sessions to an organization-defined number for all accounts and/or account types.
STIG ID: SRG-APP-000001 **Rule ID:** SV-204708r508029_rule **Vul ID:** V-204708
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation and configuration to determine if the number of concurrent sessions can be limited to the organization-defined number of sessions for all accounts and/or account types.

If a feature to limit the number of concurrent sessions is not available, is not set, or is set to unlimited, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using external Identity Provider (IdP) for authe user executes. Elasticsearch is a REST API and, as such, has no notion of sessions. Elasticsearch and Kibana do not have a connection limit.

To accomplish a connection limit, a proxy should be placed in front of the cluster.

For Elasticsearch as a SaaS product (Elastic-hosted), concurrent sessions are controlled further upstream via VPN Gateway limits (max connection of one per gateway) and by the use of Gravitational Teleport as an alternate gateway to Open SSH for managing access by Admins inside the production environment to clusters of Linux servers via SSH or the Kubernetes API.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application management includes the ability to control the number of sessions that utilize an application by all accounts and/or account types. Limiting the number of allowed sessions is helpful in limiting risks related to Denial of Service attacks.

Application servers host and expose business logic and application processes.

The application server must possess the capability to limit the maximum number of concurrent sessions in a manner that affects the entire application server or on an individual application basis.

Although there is some latitude concerning the settings themselves, the settings should follow DoD-recommended values, but the settings should be configurable to allow for future DoD direction.

While the DoD will specify recommended values, the values can be adjusted to accommodate the operational requirement of a given system.

Legacy Ids: V-35070; SV-46335

Comments:

CCI: CCI-000054The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.NIST SP 800-53 :: AC-10NIST SP 800-53A :: AC-10.1 (ii)NIST SP 800-53 Revision 4 :: AC-10

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must allocate log record storage capacity in accordance with organization-defined log record storage requirements.
STIG ID: SRG-APP-000357 **Rule ID:** SV-204788r508029_rule **Vul ID:** V-204788
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server creates log storage to buffer log data until offloading to a log data storage facility.

If the application server does not allocate storage for log data, this is a finding.

Fix Text:
Steps/Recommendation:

1. Allocate sufficient audit storage space on each of the Elastic cluster nodes to support peak demand in accordance with organization-defined audit record storage requirements.

2. Recommend creating an immediate alert to the appropriate personnel (at a minimum) when allocated log record storage volume reaches a threshold of the repository maximum log record storage capacity.

3. Elasticsearch will go into a read-only state when it detects issues with disk storage which is the most common issue affecting logging. Elasticsearch will not shutdown if logging fails for other reasons.

4. Elasticsearch should be configured so as to continue to log but cache the logs locally until log shipment can resume.

5. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Returns information about a cluster's nodes.
Request
GET /_cat/nodes

disk.total, dt, diskTotal
Total disk space, such as 458.3gb.
disk.used, du, diskUsed
Used disk space, such as 259.8gb.
disk.avail, d, disk, diskAvail
Available disk space, such as 198.4gb.
disk.used_percent, dup, diskUsedPercent
Used disk space percentage, such as 47.

6. Kibana Alerts
The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. However, it can be tailored to meet organizational needs.

Disk usage threshold
This alert is triggered when a node is nearly at disk capacity. By default, the trigger condition is set at 80 percent or more averaged over the last 5 minutes. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 1 day.

References:

a. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/current/how-monitoring-works.html
b. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/current/monitoring-overview.html
c. Kibana Alerts: https://www.elastic.co/guide/en/kibana/current/kibana-alerts.html
d. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/current/xpack-alerting.html
e. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
f. cat indices API: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-nodes.html
g. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The proper management of log records not only dictates proper archiving processes and procedures be established, it also requires allocating enough storage space to maintain the logs online for a defined period of time.

If adequate online log storage capacity is not maintained, intrusion monitoring, security investigations, and forensic analysis can be negatively affected.

It is important to keep a defined amount of logs online and readily available for investigative purposes. The logs may be stored on the application server until they can be archived to a log system or, in some instances, a Storage Area Networks (SAN). Regardless of the method used, log record storage capacity must be sufficient to store log data when the data cannot be offloaded to a log system or SAN.

Legacy Ids: V-57421; SV-71693

Comments:

CCI: CCI-001849The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.NIST SP 800-53 Revision 4 :: AU-4

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use encryption strength in accordance with the categorization of the management data during remote access management sessions.
STIG ID: SRG-APP-000014 **Rule ID:** SV-204709r508029_rule **Vul ID:** V-204709
Severity: CAT II

Documentable: No

Check Content:
Check the application server configuration to ensure all management interfaces use encryption in accordance with the management data.

If the application server is not configured to encrypt remote access management sessions in accordance with the categorization of the management data, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin

- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport

Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Remote management access is accomplished by leveraging common communication protocols and establishing a remote connection to the application server via a network for the purposes of managing the application server. If cryptography is not used, then the session data traversing the remote connection could be intercepted and compromised.

Types of management interfaces utilized by an application server include web-based HTTPS interfaces as well as command line-based management interfaces.

Legacy Ids: V-35089; SV-46376

Comments:

CCI: CCI-000068The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.NIST SP 800-53 :: AC-17 (2)NIST SP 800-53A :: AC-17 (2).1NIST SP 800-53 Revision 4 :: AC-17 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must off-load log records onto a different system or media from the system being logged.
STIG ID: SRG-APP-000358 **Rule ID:** SV-204789r508029_rule **Vul ID:** V-204789
Severity: CAT II

Documentable: No

Check Content:
Verify the log records are being off-loaded to a separate system or transferred from the application server to a storage location other than the application server itself.

The system administrator of the device may demonstrate this capability using a log

management application, system configuration, or other means.

If logs are not being off-loaded, this is a finding.

Fix Text:
Steps/Recommendation:

1. Setup appropriate lifecycle for the indices and create snapshots.

2. Elasticsearch can be configured to off-load log records onto a different system or media from the system being logged.

References:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/current/resiliency.html
b. Manage the index lifecycle:
https://www.elastic.co/guide/en/elasticsearch/reference/current/index-lifecycle-management.html
c. Automate snapshots with SLM:
https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshots-take-snapshot.html#automate-snapshots-slm

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, filenames involved, access control or flow control rules invoked.

Off-loading is a common process in information systems with limited log storage capacity.

Centralized management of log records provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records. Application servers and their related components are required to off-load log records onto a different system or media than the system being logged.

Legacy Ids: V-57423; SV-71695

Comments:

CCI: CCI-001851The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.NIST SP 800-53 Revision 4 :: AU-4 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must implement cryptography mechanisms to protect the integrity of the remote access session.
STIG ID: SRG-APP-000015 **Rule ID:** SV-204710r508029_rule **Vul ID:** V-204710
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to ensure the application server is configured to use cryptography to protect the integrity of remote access sessions.

If the application server is not configured to implement cryptography mechanisms to protect the integrity of remote access sessions, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features

are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:

https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Encryption is critical for protection of remote access sessions. If encryption is not being used for integrity, malicious users may gain the ability to modify the application server configuration. The use of cryptography for ensuring integrity of remote access sessions mitigates that risk.

Application servers utilize a web management interface and scripted commands when allowing remote access. Web access requires the use of TLS and scripted access requires using ssh or some other form of approved cryptography. Application servers must have a capability to enable a secure remote admin capability.

FIPS 140-2 approved TLS versions must be enabled and non-FIPS-approved SSL versions must be disabled.

NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-35090; SV-46377

Comments:

CCI: CCI-001453The information system implements cryptographic mechanisms to protect the integrity of remote access sessions.NIST SP 800-53 :: AC-17 (2)NIST SP 800-53A :: AC-17 (2).1NIST SP 800-53 Revision 4 :: AC-17 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide an immediate warning to the SA and ISSO, at a minimum, when allocated log record storage volume reaches 75% of maximum log record storage capacity.
STIG ID: SRG-APP-000359 **Rule ID:** SV-204790r508029_rule **Vul ID:** V-204790

Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server logging system provides a warning to the SA and ISSO when 75% of allocated log record storage volume is reached.

If designated alerts are not sent, or the application server is not configured to use a dedicated logging tool that meets this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

Recommend setting up an alert to the SA and ISSO, at a minimum, when allocated log record storage volume reaches 75% of maximum log record storage capacity.

1. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Recommend using Machine Learning to identify anomalies in an environment to reduce the manual steps required to create individual alerts.

3. Metricbeat is the recommended method for collecting and shipping monitoring data to a monitoring cluster.

4. After collecting monitoring data for one or more products in the Elastic Stack, Kibana can be configured to retrieve that information and display it in on the Stack Monitoring page.

5. At a minimum, capture monitoring data for the Elasticsearch production cluster. Once that data exists, Kibana can display monitoring data for other products in the cluster.

6. Identify where to retrieve monitoring data from. The cluster that contains the monitoring data is referred to as the monitoring cluster. If the monitoring data is stored on a dedicated monitoring cluster, it is accessible even when the cluster monitoring is not.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

7. By default, data is retrieved from the cluster specified in the elasticsearch.hosts value in the

kibana.yml file.

8. If the Elastic security features are enabled on the monitoring cluster, configure a user ID and password so Kibana can retrieve the data.
- Create a user that has the monitoring_user built-in role on the monitoring cluster.
- Add the xpack.monitoring.elasticsearch.username and xpack.monitoring.elasticsearch.password settings in the kibana.yml file. If these settings are omitted, Kibana uses the elasticsearch.username and elasticsearch.password setting values.

9. If the Elastic security features are enabled on the Kibana server, only users that have the authority to access Kibana indices and to read the monitoring indices can use the monitoring dashboards.
- These users must exist on the monitoring cluster. When accessing a remote monitoring cluster, use credentials that are valid on both the Kibana server and the monitoring cluster.
- Create users that have the monitoring_user and kibana_admin built-in roles.

10. Open Kibana in your web browser.
By default, go to http://localhost:5601/.
If the Elastic security features are enabled, log in.

11. In the side navigation, click Stack Monitoring.
If data collection is disabled, a prompt will be displayed to turn on data collection. If Elasticsearch security features are enabled, manage cluster privileges are needed to turn on data collection.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Use the cat indices API to get the following information for each index in a cluster:
- Shard count
- Document count
- Deleted document count
- Primary store size
- Total store size of all shards, including shard replicas

These metrics are retrieved directly from Lucene, which Elasticsearch uses internally to power indexing and search. As a result, all document counts include hidden nested documents.

To get an accurate count of Elasticsearch documents, use the cat count or count APIs.

References:
a. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/configuring-monitoring.html
b. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/monitoring-data.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. cat indices API:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process logs as required. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. Notification of the storage condition will allow administrators to take actions so that logs are not lost. This requirement can be met by configuring the application server to utilize a dedicated logging tool that meets this requirement.

Legacy Ids: V-57427; SV-71699

Comments:

CCI: CCI-001855The information system provides a warning to organization-defined personnel, roles and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.NIST SP 800-53 Revision 4 :: AU-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must ensure remote sessions for accessing security functions and security-relevant information are logged.
STIG ID: SRG-APP-000016 **Rule ID:** SV-204711r508029_rule **Vul ID:** V-204711
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation to determine if the application server logs remote administrative sessions.

If the application server does not log remote sessions for the admin user, then this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to log an event for each instance when the administrator accesses the system remotely.

1. Elasticsearch can preform audit logging. Enable the audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log an event for each instance when the administrator accesses the system remotely.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Logging must be utilized in order to track system activity, assist in diagnosing system issues, and provide evidence needed for forensic investigations post security incident.

Remote access by administrators requires that the admin activity be logged.

Application servers provide a web and command line-based remote management capability for managing the application server. Application servers must ensure that all actions related to administrative functionality such as application server configuration are logged.

Legacy Ids: V-57411; SV-71683

Comments:

CCI: CCI-000067The information system monitors remote access methods.NIST SP 800-53 :: AC-17 (1)NIST SP 800-53A :: AC-17 (1).1NIST SP 800-53 Revision 4 :: AC-17 (1)

Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide an immediate real-time alert to authorized users of all log failure events requiring real-time alerts.
STIG ID: SRG-APP-000360 **Rule ID:** SV-204791r508029_rule **Vul ID:** V-204791
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log system provides a real-time alert to authorized users when log failure events occur requiring real-time alerts.

If designated alerts are not sent to authorized users, this is a finding.

Fix Text:
Steps/Recommendation:

Recommend setting up an alert to the SA and ISSO, at a minimum, when allocated log record storage volume reaches 75% of maximum log record storage capacity.

1. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Recommend using Machine Learning to identify anomalies in an environment to reduce the manual steps required to create individual alerts.

3. Metricbeat is the recommended method for collecting and shipping monitoring data to a monitoring cluster.

4. After collecting monitoring data for one or more products in the Elastic Stack, Kibana can be configured to retrieve that information and display it in on the Stack Monitoring page.

5. At a minimum, capture monitoring data for the Elasticsearch production cluster. Once that data exists, Kibana can display monitoring data for other products in the cluster.

6. Identify where to retrieve monitoring data from. The cluster that contains the monitoring data is referred to as the monitoring cluster. If the monitoring data is stored on a dedicated monitoring cluster, it is accessible even when the cluster monitoring is not.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see

https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

7. By default, data is retrieved from the cluster specified in the elasticsearch.hosts value in the kibana.yml file.

8. If the Elastic security features are enabled on the monitoring cluster, configure a user ID and password so Kibana can retrieve the data.
- Create a user that has the monitoring_user built-in role on the monitoring cluster.
- Add the xpack.monitoring.elasticsearch.username and xpack.monitoring.elasticsearch.password settings in the kibana.yml file. If these settings are omitted, Kibana uses the elasticsearch.username and elasticsearch.password setting values.

9. If the Elastic security features are enabled on the Kibana server, only users that have the authority to access Kibana indices and to read the monitoring indices can use the monitoring dashboards.
- These users must exist on the monitoring cluster. When accessing a remote monitoring cluster, use credentials that are valid on both the Kibana server and the monitoring cluster.
- Create users that have the monitoring_user and kibana_admin built-in roles.

10. Open Kibana in your web browser.
By default, go to http://localhost:5601/.
If the Elastic security features are enabled, log in.

11. In the side navigation, click Stack Monitoring.
If data collection is disabled, a prompt will be displayed to turn on data collection. If Elasticsearch security features are enabled, manage cluster privileges are needed to turn on data collection.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Use the cat indices API to get the following information for each index in a cluster:
- Shard count
- Document count
- Deleted document count
- Primary store size
- Total store size of all shards, including shard replicas

These metrics are retrieved directly from Lucene, which Elasticsearch uses internally to power indexing and search. As a result, all document counts include hidden nested documents.

To get an accurate count of Elasticsearch documents, use the cat count or count APIs.

References:

a. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/configuring-monitoring.html
b. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/monitoring-data.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. cat indices API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process logs as required. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. Notification of the failure event will allow administrators to take actions so that logs are not lost.

Legacy Ids: V-57429; SV-71701

Comments:

CCI: CCI-001858The information system provides a real-time alert in organization-defined real-time period to organization-defined personnel, roles and/or locations when organization-defined audit failure events requiring real-time alerts occur.NIST SP 800-53 Revision 4 :: AU-5 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
STIG ID: SRG-APP-000033 **Rule ID:** SV-204712r508029_rule **Vul ID:** V-204712
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and configuration to determine if the system enforces authorization requirements for logical access to the system in accordance with applicable policy.

If the application server is not configured to utilize access controls or follow access control policies, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:
a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Strong access controls are critical to securing the application server. Access

control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) must be employed by the application server to control access between users (or processes acting on behalf of users) and objects (e.g., applications, files, records, processes, application domains) in the application server.

Without stringent logical access and authorization controls, an adversary may have the ability, with very little effort, to compromise the application server and associated supporting infrastructure.

Legacy Ids: V-35738; SV-47025

Comments:

CCI: CCI-000213The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.NIST SP 800-53 :: AC-3NIST SP 800-53A :: AC-3.1NIST SP 800-53 Revision 4 :: AC-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must compare internal application server clocks at least every 24 hours with an authoritative time source.
STIG ID: SRG-APP-000371 **Rule ID:** SV-204792r508029_rule **Vul ID:** V-204792
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and confirm that the application server compares internal application server clocks at least every 24 hours with an authoritative time source.

If the application server does not compare internal application server clocks to an authoritative source or if the frequency is greater than every 24 hours, this is a finding.

Fix Text:
Stp/3Recommendation:

1. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index.

date {
match =>; ...
time zone =>; "%{tz}"; # or the defined field name
}

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/master/add-locale.html
c. Ingest processor reference:
https://www.elastic.co/guide/en/elasticsearch/reference/master/processors.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronization of system clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. To meet this requirement, the organization will define an authoritative time source and have each system compare its internal clock at least every 24 hours.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57435; SV-71707

Comments:

CCI: CCI-001891The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

Rule Title: The application server management interface must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.
STIG ID: SRG-APP-000068 **Rule ID:** SV-204713r508029_rule **Vul ID:** V-204713
Severity: CAT II

Documentable: No

Check Content:
Review the application server management interface configuration to verify the application server is configured to display the Standard Mandatory DoD Notice and Consent Banner before granting access.

The banner must read:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

If the application server management interface does not display the banner or displays an unapproved banner, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch natively does not provide a GUI interface to display the DoD Notice. Kibana can be used as the front end, to perform this configuration. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to perform this configuration. The recommendation is to integrate Elasticsearch with these services to display the Standard Mandatory DoD Notice and Consent

Banner before granting access to the Application Server.

References:
a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers are required to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system management interface, providing privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance that states that:

(i) users are accessing a U.S. Government information system;
(ii) system usage may be monitored, recorded, and subject to audit;
(iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
(iv) the use of the system indicates consent to monitoring and recording.

System use notification messages can be implemented in the form of warning banners displayed when individuals log on to the information system.

System use notification is intended only for information system access including an

interactive logon interface with a human user, and is not required when an interactive interface does not exist.

Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Legacy Ids: V-35096; SV-46383

Comments:

CCI: CCI-000048The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.NIST SP 800-53 :: AC-8 aNIST SP 800-53A :: AC-8.1 (ii)NIST SP 800-53 Revision 4 :: AC-8 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server management interface must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.

STIG ID: SRG-APP-000069 **Rule ID:** SV-204714r508029_rule **Vul ID:** V-204714
Severity: CAT II

Documentable: No

Check Content:
Review application server management interface product documentation and configuration to determine that the logon banner can be displayed until the user takes action to acknowledge the agreement.

If the banner screen allows continuation to the application server without user interaction, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch natively does not provide a GUI interface to display the DoD Notice. Kibana can be used as the front end, to perform this configuration. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to perform this configuration. The recommendation is to integrate Elasticsearch with these services to retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.

References:
a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To establish acceptance of system usage policy, a click-through banner at the application server management interface logon is required. The banner shall prevent further activity on the application server unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35098; SV-46385

Comments:

CCI: CCI-000050The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.NIST SP 800-53 :: AC-8 bNIST SP 800-53A :: AC-8.1 (iii)NIST SP 800-53 Revision 4 :: AC-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must synchronize internal application server clocks to an authoritative time source when the time difference is greater than the organization-defined time period.
STIG ID: SRG-APP-000372 **Rule ID:** SV-204793r508029_rule **Vul ID:** V-204793
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server is configured to reset internal information clocks when the difference is greater than a defined threshold with an authoritative time source.

If the application server cannot synchronize internal application server clocks to the authoritative time source when the time difference is greater than the organization-defined time period, this is a finding.

Fix Text:
Step/Recommendation:

1. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index.

date {
match =>; ...
time zone =>; "%{tz}"; # or the defined field name
}

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/master/add-locale.html
c. Ingest processor reference:
https://www.elastic.co/guide/en/elasticsearch/reference/master/processors.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronization of internal application server clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. To meet this requirement, the organization will define an authoritative time source and have each system synchronize when the time difference is greater than a defined time period. The industry standard for the threshold is 1ms.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or

a hybrid with another control provider.

Legacy Ids: V-57437; SV-71709

Comments:

CCI: CCI-002046The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.NIST SP 800-53 Revision 4 :: AU-8 (1) (b)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.
STIG ID: SRG-APP-000080 **Rule ID:** SV-204715r508029_rule **Vul ID:** V-204715
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and server configuration to determine if the system does protect against an individual's (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

If the application does not meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:
a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html
i. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Non-repudiation of actions taken is required in order to maintain application integrity. Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message.

Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document.

Typical application server actions requiring non-repudiation will be related to application deployment among developers/users and administrative actions taken by admin personnel.

Legacy Ids: V-35135; SV-46422

Comments:

CCI: CCI-000166The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.NIST SP 800-53 :: AU-10NIST SP 800-53A :: AU-10.1NIST SP 800-53 Revision 4 :: AU-10

Rule Title: For application servers providing log record aggregation, the application server must compile log records from organization-defined information system components into a system-wide log trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail.
STIG ID: SRG-APP-000086 **Rule ID:** SV-204716r508029_rule **Vul ID:** V-204716
Severity: CAT II

Documentable: No

Check Content:
Review the application server log feature configuration to determine if the application server or an external logging tool in conjunction with the application server does compile log records from multiple components within the server into a system-wide log trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. All applications should capture the time of log/event creation.

Note: Elasticsearch architecture is designed to collect log records from multiple components within the server into a system-wide log trail.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.
date {
match =>; ...
time zone =>; "%{tz}"; # or whatever you call the field
}

4. To verify if the ingest pipeline is setup to capture the time, use the following: GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. For Time in host machine: https://chrony.tuxfamily.org/

b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/8.0/add-locale.html
c. Processors:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest-processors.html
d. Ingest node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html
e. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/date-processor.html
f. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/get-pipeline-api.html
g. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
h. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
i. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log generation and log records can be generated from various components within the application server. The list of logged events is the set of events for which logs are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating log records (e.g., logable events, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked).

The events occurring must be time-correlated in order to conduct accurate forensic analysis. In addition, the correlation must meet certain tolerance criteria. For instance, DoD may define that the time stamps of different logged events must not differ by any amount greater than ten seconds. It is also acceptable for the application server to utilize an external logging tool that provides this capability.

Legacy Ids: V-35139; SV-46426

Comments:

CCI: CCI-000174The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.NIST SP 800-53 :: AU-12 (1)NIST SP 800-53A :: AU-12 (1).1 (iii&v)NIST SP 800-53 Revision 4 :: AU-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must record time stamps for log records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).
STIG ID: SRG-APP-000374 **Rule ID:** SV-204794r508029_rule **Vul ID:** V-204794
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration files to determine if time stamps for log records can be mapped to UTC or GMT.

If the time stamp cannot be mapped to UTC or GMT, this is a finding.

Fix Text:
Steps/Recommendation:

Elasticsearch architecture is designed to collect log records from multiple components within the server into a system-wide log trail.

1. All applications should capture the time of log/event creation.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Setup all the host/device to use UTC time zone (or GMT as per the business requirement), use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index.

```
date {
match =>; ...
time zone =>; "%{tz}"; # or the defined field name
}
```

4. To verify if the ingest pipeline is setup to capture the time, use the following: GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:

https://www.elastic.co/guide/en/beats/filebeat/master/add-locale.html
c. Ingestor processor reference:
https://www.elastic.co/guide/en/elasticsearch/reference/master/processors.html
d. Ingest node: https://www.elastic.co/guide/en/elasticsearch/reference/master/ingest.html
e. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/master/date-processor.html
f. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/master/get-pipeline-api.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the application include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57431; SV-71703

Comments:

CCI: CCI-001890The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).NIST SP 800-53 Revision 4 :: AU-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records for access and authentication events.
STIG ID: SRG-APP-000089 **Rule ID:** SV-204717r508029_rule **Vul ID:** V-204717
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the deployed system configuration to determine if, at a minimum, system startup and shutdown, system access, and system authentication events are logged.

If the logs do not include the minimum logable events, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to generate log records for system startup and shutdown, system access, and system authentication events.

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log for system startup and shutdown, system access, and system authentication events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html

c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Starting Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/starting-elasticsearch.html
o. Stopping Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/stopping-elasticsearch.html
p. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
q. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html
r. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log records can be generated from various components within the application server. From an application server perspective, certain specific application server functionalities may be logged as well. The application server must allow the definition of what events are to be logged. As conditions change, the number and types of events to be logged may change, and the application server must be able to facilitate these changes.

The minimum list of logged events should be those pertaining to system startup and shutdown, system access, and system authentication events.

Legacy Ids: V-35141; SV-46428

Comments:

CCI: CCI-000169The information system provides audit record generation capability for the auditable events defined in AU-2 a at organization-defined information system components.NIST SP 800-53 :: AU-12 aNIST SP 800-53A :: AU-12.1 (ii)NIST SP 800-53 Revision 4 :: AU-12 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must record time stamps for log records that meet a granularity of one second for a minimum degree of precision.
STIG ID: SRG-APP-000375 **Rule ID:** SV-204795r508029_rule **Vul ID:** V-204795
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration files to determine if time stamps for log records meet a granularity of one second.

If the time stamp cannot generate to a one-second granularity, this is a finding.

Fix Text:
Steps/Recommendation:

1. In JSON, dates are represented as strings. Elasticsearch uses a set of preconfigured formats to recognize and parse these strings into a long value representing milliseconds-since-the-epoch in UTC.

2. Elastic Stack's UI (Kibana) can also be utilized to search records that meet a granularity of one second for a minimum degree of precision.

Reference:

a. Mapping date format:
https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-date-format.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To investigate an incident, the log records should be easily put into chronological order. Without sufficient granularity of time stamps, the chronological order cannot be determined.

Time stamps generated by the application server include date and time. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks.

Legacy Ids: V-57433; SV-71705

Comments:

CCI: CCI-001889The information system records time stamps for audit records that meets organization-defined granularity of time measurement.NIST SP 800-53 Revision 4 :: AU-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must allow only the ISSM (or individuals or roles appointed by the ISSM) to select which logable events are to be logged.
STIG ID: SRG-APP-000090 **Rule ID:** SV-204718r508029_rule **Vul ID:** V-204718
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and configuration to determine if the system only allows the ISSM (or individuals or roles appointed by the ISSM) to change logable events.

If the system is not configured to perform this function, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a specified format.

3. Recommend using an external Identity Management system for authentication of users. Then use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

4. If users are authenticated with the native or file realms, role assignment can be managed using the user management APIs or the users command-line tool (elasticsearch-users), respectively.

Role-mappings can be defined via an API or managed through files. These two sources of role-mapping are combined inside the Elasticsearch security features, so it is possible for a single user to have some Roles mapped through the API and other Roles mapped through files.

Role-mappings must be created for other types of realms that define which Roles should be assigned to each user based on their username, groups, or other metadata.

References:

a. Elasticsearch authentication:
https://www.elastic.co/blog/a-deep-dive-into-elasticsearch-authentication-realms
b. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
c. Role-based access control (RBAC) in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
d. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
e. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
f. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
g. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
h. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
i. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
j. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
k. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
l. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
m. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
n. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
o. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
p. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html

q. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
r. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
s. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log records can be generated from various components within the application server, (e.g., httpd, beans, etc.) From an application perspective, certain specific application functionalities may be logged, as well.

The list of logged events is the set of events for which logs are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating log records (e.g., logable events, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked).

Application servers utilize role-based access controls in order to specify the individuals who are allowed to configure application component logable events. The application server must be configured to select which personnel are assigned the role of selecting which logable events are to be logged.

The personnel or roles that can select logable events are only the ISSM (or individuals or roles appointed by the ISSM).

Legacy Ids: V-35142; SV-46429

Comments:

CCI: CCI-000171The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system.NIST SP 800-53 :: AU-12 bNIST SP 800-53A :: AU-12.1 (iii)NIST SP 800-53 Revision 4 :: AU-12 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must enforce access restrictions associated with changes

to application server configuration.
STIG ID: SRG-APP-000380 **Rule ID:** SV-204796r508029_rule **Vul ID:** V-204796
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the system employs mechanisms to enforce restrictions on application server configuration changes.

Configuration changes include, but are not limited to, automatic code deployments, software library updates, and changes to configuration settings within the application server.

If the application server does not enforce access restrictions for configuration changes, this is a finding.

Fix Text:
Steps/Recommendation:

1.For on-premises implementation, the Elasticsearch system does not prevent modifications on the software resident within software libraries.

Configure the application OS file permissions to enforce access restrictions associated with changes to the application server configuration to include code deployment, library updates, and changes to application server configuration settings.

2. For the hosted Elasticsearch Service (SaaS offering), only an Elastic Admin with access to the Infrastructure as Code files would be able to modify files and modules that cannot be configured directly by the Customer. The Customer is responsible for a secure configuration with Role-based access control (RBAC) controls. Elastic monitors for such changes in the hosted production environment and investigates if detected.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When dealing with access restrictions pertaining to change control, it should be noted that any changes to the software, and/or application server configuration can potentially have significant effects on the overall security of the system.

Access restrictions for changes also include application software libraries.

If the application server provides automatic code deployment capability, (where updates to applications hosted on the application server are automatically performed, usually by the developers' IDE tool), it must also provide a capability to restrict the use of automatic application deployment. Automatic code deployments are allowable in a development environment, but not in production.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57491; SV-71767

Comments:

CCI: CCI-001813The information system enforces access restrictions.NIST SP 800-53 Revision 4 :: CM-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful attempts to access subject privileges occur.
STIG ID: SRG-APP-000091 **Rule ID:** SV-204719r508029_rule **Vul ID:** V-204719
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when successful/unsuccessful attempts are made to access privileges.

If log records are not generated, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to generate log records when privileges are successfully/unsuccessfully accessed.

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log records when privileges are successfully/unsuccessfully accessed.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Accessing a subject's privileges can be used to elevate a lower-privileged subject's privileges temporarily in order to cause harm to the application server or to gain privileges to operate temporarily for a designed purpose. When these actions take place, the event needs to be logged.

Application servers either provide a local user store, or they integrate with enterprise user stores like LDAP. When the application server provides the user store and enforces authentication, the application server must generate a log record when modification of privileges is successfully or unsuccessfully performed.

Legacy Ids: V-35143; SV-46430

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must log the enforcement actions used to restrict access associated with changes to the application server.

STIG ID: SRG-APP-000381 **Rule ID:** SV-204797r508029_rule **Vul ID:** V-204797
Severity: CAT II

Documentable: No

Check Content:
Check the application server documentation and logs to determine if enforcement actions used to restrict access associated with changes to the application server are logged.

If these actions are not logged, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, configure the application OS to log the enforcement actions used to restrict access associated with changes to the application server filesystem.

2. For the hosted Elasticsearch Service (SaaS offering), only an Elastic Admin with access to the Infrastructure as Code files would be able to modify files and modules that cannot be configured directly by Customer. Customer is responsible for secure configuration with Role-based access control (RBAC) controls. Elastic monitors for such changes in the hosted production environment and investigates if detected.

3. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

Note: If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

4. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

5. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log the enforcement actions used to restrict access associated with changes to the application server

fiesystem.

6. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes. For example, the Elasticsearch directory contents include among others:

LICENSE.txt, NOTICE.txt, README.asciidoc, bin, config, data, jdk, lib, logs, modules, plugins

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n.Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without logging the enforcement of access restrictions against changes to the application server configuration, it will be difficult to identify attempted attacks, and a log trail will not be available for forensic investigation for after-the-fact actions. Configuration changes may occur to any of the modules within the application server through the management interface, but logging of actions to the configuration of a module outside the application server is not logged.

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. Enforcement action methods may be as simple as denying access to a file based on the application of file permissions (access restriction). Log items may consist of lists of actions blocked by access restrictions or changes identified after the fact.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57493; SV-71769

Comments:

CCI: CCI-001814The Information system supports auditing of the enforcement actions.NIST SP 800-53 Revision 4 :: CM-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must initiate session logging upon startup.
STIG ID: SRG-APP-000092 **Rule ID:** SV-204720r508029_rule **Vul ID:** V-204720
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation and server configuration to determine if the application server initiates session logging on application server startup.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:

Steps/Recommendation:

1. By enabling Set xpack.security.audit.enabled to true in elasticsearch.yml for each cluster node, Elastic starts up auditing when the node is started.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) which must be configured to initiate session logging upon startup.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Session logging activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Legacy Ids: V-35148; SV-46435

Comments:

CCI: CCI-001464The information system initiates session audits at system start-up.NIST SP 800-53 :: AU-14 (1)NIST SP 800-53A :: AU-14 (1).1NIST SP 800-53 Revision 4 :: AU-14 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must require users to re-authenticate when organization-defined circumstances or situations require re-authentication.
STIG ID: SRG-APP-000389 **Rule ID:** SV-204798r508029_rule **Vul ID:** V-204798
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server requires a user to re-authenticate when organization-defined circumstances or situations are met.

If the application server does not require a user to re-authenticate when organization-defined circumstances or situations are met, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to require a user to re-authenticate when organization-defined circumstances or situations are met.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout

Ensures that user sessions will expire after a period of inactivity. This and xpack.security.session.lifespan are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.lifespan

Ensures that user sessions will expire after the defined time period. This behavior is also known as an "absolute timeout". If this is not set, user sessions could stay active indefinitely. This and xpack.security.session.idleTimeout are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.cleanupInterval

Sets the interval at which Kibana tries to remove expired and invalid sessions from the session index. By default, this value is 1 hour. The minimum value is 10 seconds.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When applications provide the capability to change security roles or escalate the functional capability of the application, it is critical the user re-authenticate.

In addition to the re-authentication requirements associated with session locks, the application server security model may require re-authentication of individuals in other situations, including (but not limited to) the following circumstances:

(i) When authenticators change;
(ii) When roles change;
(iii) When security categories of information systems change;
(iv) When the execution of privileged functions occurs;
(v) After a fixed period of time; or
(vi) Periodically.

Within the DoD, the minimum circumstances requiring re-authentication are privilege escalation and role changes.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57523; SV-71799

Comments:

CCI: CCI-002038The organization requires users to reauthenticate when organization-defined circumstances or situations requiring reauthentication.NIST SP 800-53 Revision 4 :: IA-11

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing information to establish what type of events occurred.
STIG ID: SRG-APP-000095 **Rule ID:** SV-204721r508029_rule **Vul ID:** V-204721
Severity: CAT II

Documentable: No

Check Content:
Review the application server log configuration to determine if the application server produces log records showing what type of event occurred.

If the log data does not show the type of event, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish what type of events occurred. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat

s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
w. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Without being able to establish what type of event occurred, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible.

Log record content that may be necessary to satisfy the requirement of this control includes time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Application servers must log all relevant log data that pertains to the application server. Examples of relevant data include, but are not limited to, Java Virtual Machine (JVM) activity, HTTPD/Web server activity, and application server-related system process activity.

Legacy Ids: V-35159; SV-46446

Comments:

CCI: CCI-000130The information system generates audit records containing information that establishes what type of event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must require devices to re-authenticate when organization-defined circumstances or situations require re-authentication.
STIG ID: SRG-APP-000390 **Rule ID:** SV-204799r508029_rule **Vul ID:** V-204799
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server requires devices to re-authenticate when organization-defined circumstances or situations require re-authentication.

If the application server does not require a device to re-authenticate, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to require devices to re-authenticate when organization-defined circumstances or situations are met.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout

Ensures that user sessions will expire after a period of inactivity. This and xpack.security.session.lifespan are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.lifespan

Ensures that user sessions will expire after the defined time period. This behavior also known as an "absolute timeout". If this is not set, user sessions could stay active indefinitely. This and xpack.security.session.idleTimeout are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.cleanupInterval

Sets the interval at which Kibana tries to remove expired and invalid sessions from the session index. By default, this value is 1 hour. The minimum value is 10 seconds.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g., 20m, 24h, 7d, 1w).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without re-authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of devices, including (but not limited to), the following other situations.

(i) When authenticators change;
(ii) When roles change;
(iii) When security categories of information systems change;
(iv) After a fixed period of time; or
(v) Periodically.

For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification decisions (as opposed to the actual identifiers) to the services that need to act on those decisions.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57525; SV-71801

Comments:

CCI: CCI-002039The organization requires devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.NIST SP 800-53 Revision 4 :: IA-11

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing sufficient information to establish when (date and time) the events occurred.
STIG ID: SRG-APP-000096 **Rule ID:** SV-204722r508029_rule **Vul ID:** V-204722
Severity: CAT II

Documentable: No

Check Content:
Review the logs on the application server to determine if the date and time are included in the log event data.

If the date and time are not included, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, @timestamp has to be captured.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish when the events occurred. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
w. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
x. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct order of the events that occurred is important during forensic analysis. Events that appear harmless by themselves might be flagged as a potential threat when properly viewed in sequence. By also establishing the event date and time, an event can be properly viewed with an enterprise tool to fully see a possible threat in its entirety.

Without sufficient information establishing when the log event occurred, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, file names involved, access control, or flow control rules invoked.

In addition to logging event information, application servers must also log the corresponding dates and times of these events. Examples of event data include, but are not limited to, Java Virtual Machine (JVM) activity, HTTPD activity, and application server-related system process activity.

Legacy Ids: V-35165; SV-46452

Comments:

CCI: CCI-000131The information system generates audit records containing information that establishes when an event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must accept Personal Identity Verification (PIV) credentials to access the management interface.
STIG ID: SRG-APP-000391 **Rule ID:** SV-204800r508029_rule **Vul ID:** V-204800
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to ensure the application server accepts PIV credentials to the management interface.

If PIV credentials are not accepted, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides Personal Identity Verification (PIV) credentials to access the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

PIV credentials are only used in an unclassified environment.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12, as well as its use as a primary component of layered protection for national security systems.

The application server must support the use of PIV credentials to access the management interface and perform management functions.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57503; SV-71779

Comments:

CCI: CCI-001953The information system accepts Personal Identity Verification (PIV) credentials.NIST SP 800-53 Revision 4 :: IA-2 (12)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing sufficient information to establish where the events occurred.

STIG ID: SRG-APP-000097 **Rule ID:** SV-204723r508029_rule **Vul ID:** V-204723
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings on the application server to determine if the application server is configured to log information that establishes where within the application server the event occurred.

The data in the log file should identify the event, the component, module, filename, host name, servlets, containers, APIs, or other functionality within the application server, as well as, any source and destination information that indicates where an event occurred.

If the application server is not configured to log where within the application server the event took place, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, node.name, node.id, host.ip, host.name, origin.address, origin.type, has to be captured.

5. For event.type equal to transport, then extra attributes should be captured: action, indices, request.name

6. For event.type equal to ip_filter, transport_profile and rule should be captured.

7. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish where the events occurred. Fleet managed Elastic Agents

can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the

Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct location or process within the application server where the events occurred is important during forensic analysis. To determine where an event occurred, the log data must contain information that identifies the source and destination of the events such as application components, modules, filenames, host names, servlets, containers, APIs, and other functionality.

Legacy Ids: V-35167; SV-46454

Comments:

CCI: CCI-000132The information system generates audit records containing information that establishes where the event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must electronically verify Personal Identity Verification (PIV) credentials for access to the management interface.
STIG ID: SRG-APP-000392 **Rule ID:** SV-204801r508029_rule **Vul ID:** V-204801
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to ensure the application server electronically verifies PIV credentials to the management interface.

If PIV credentials are not electronically verified, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which must electronically verify Personal Identity Verification (PIV) credentials for access to the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The use of Personal Identity Verification (PIV) credentials facilitates standardization and reduces the risk of unauthorized access.

PIV credentials are only used in an unclassified environment.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12, as well as its use as a primary component of layered protection for national security systems.

The application server must electronically verify the use of PIV credentials to access the management interface and perform management functions.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57505; SV-71781

Comments:

CCI: CCI-001954The information system electronically verifies Personal Identity Verification (PIV) credentials.NIST SP 800-53 Revision 4 :: IA-2 (12)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records containing sufficient information to establish the sources of the events.
STIG ID: SRG-APP-000098 **Rule ID:** SV-204724r508029_rule **Vul ID:** V-204724
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployment configuration to determine if the application server is configured to generate sufficient information to resolve the source, e.g., source IP, of the log event.

Request a user access the application server and generate logable events, and then review the logs to determine if the source of the event can be established.

If the source of the event cannot be determined, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, node.name, node.id, host.ip, host.name, origin.address, origin.type, has to be captured.

5. For event.type equal to transport, then extra attributes should be captured: action, indices, request.name

6. For event.type equal to ip_filter, transport_profile and rule should be captured.

7. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish the source of the events. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash

t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct source, e.g., source IP, of the events is important during forensic analysis. Correctly determining the source will add information to the overall reconstruction of the logable event. By determining the source of the event correctly, analysis of the enterprise can be undertaken to determine if the event compromised other assets within the enterprise.

Without sufficient information establishing the source of the logged event, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, file names involved, access control, or flow control rules invoked.

Legacy Ids: V-35170; SV-46457

Comments:

CCI: CCI-000133The information system generates audit records containing information that establishes the source of the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prohibit the use of cached authenticators after an organization-defined time period.
STIG ID: SRG-APP-000400 **Rule ID:** SV-204804r508029_rule **Vul ID:** V-204804

Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server prohibits the use of cached authenticators after an organization-defined timeframe.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and authenticate users. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which prohibit the use of cached authenticators after an organization-defined time period.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When the application server is using PKI authentication, a local revocation cache must be stored for instances when the revocation cannot be authenticated through the network, but if cached authentication information is out of date, the validity of the authentication information may be questionable.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57513; SV-71789

Comments:

CCI: CCI-002007The information system prohibits the use of cached authenticators after an organization defined time period.NIST SP 800-53 Revision 4 :: IA-5 (13)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must produce log records that contain sufficient information to establish the outcome of events.
STIG ID: SRG-APP-000099 **Rule ID:** SV-204725r508029_rule **Vul ID:** V-204725
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and the log files on the application server to determine if the logs contain information that establishes the outcome of event data.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When

audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. event.action captures the type of event that occurred: anonymous_access_denied, authentication_failed, authentication_success, realm_authentication_failed, access_denied, access_granted, connection_denied, connection_granted, tampered_request, run_as_denied, or run_as_granted.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish the outcome of the events. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, filenames involved, access control or flow control rules invoked.

Success and failure indicators ascertain the outcome of a particular application server event or function. As such, they also provide a means to measure the impact of an event and help authorized personnel to determine the appropriate response. Event outcome may also include event-specific results (e.g., the security state of the information system after the event occurred).

Legacy Ids: V-35176; SV-46463

Comments:

CCI: CCI-000134The information system generates audit records containing information that establishes the outcome of the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

Rule Title: The application server, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.
STIG ID: SRG-APP-000401 **Rule ID:** SV-204805r508029_rule **Vul ID:** V-204805
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server provides a PKI integration capability that implements a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) that implements a local cache of revocation data to support path discovery and validation to manage accounts and authenticate users. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides multi-factor authentication. The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The cornerstone of the PKI is the private key used to encrypt or digitally sign information. The key by itself is a cryptographic value that does not contain specific user information.

Application servers must provide the capability to utilize and meet requirements of the DoD Enterprise PKI infrastructure for application authentication, but without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates) when access through the network to the CA is not available.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57511; SV-71787

Comments:

CCI: CCI-001991The information system for PKI-based authentication implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.NIST SP 800-53 Revision 4 :: IA-5 (2) (d)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records containing information that establishes the identity of any individual or process associated with the event.
STIG ID: SRG-APP-000100 **Rule ID:** SV-204726r508029_rule **Vul ID:** V-204726
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and the log files on the application server to determine if the logs contain information that establishes the identity of the user or process associated with log event data.

If the application server does not produce logs that establish the identity of the user or process associated with log event data, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. event.action captures the type of event that occurred: anonymous_access_denied, authentication_failed, authentication_success, realm_authentication_failed, access_denied, access_granted, connection_denied, connection_granted, tampered_request, run_as_denied, or run_as_granted.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information that establishes the identity of any individual or process associated with the event. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes: time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Application servers have differing levels of logging capabilities that can be specified by setting a verbosity level. The application server must, at a minimum, be capable of establishing the identity of any user or process that is associated with any particular event.

Legacy Ids: V-35182; SV-46469

Comments:

CCI: CCI-001487The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must accept Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.
STIG ID: SRG-APP-000402 **Rule ID:** SV-204806r508029_rule **Vul ID:** V-204806
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server accepts PIV credentials from other federal agencies to access the management interface.

If the application server does not accept other federal agency PIV credentials to access the management interface, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html

e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. PIV credentials are only used in an unclassified environment.

Access may be denied to authorized users if federal agency PIV credentials are not accepted to access the management interface.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57515; SV-71791

Comments:

CCI: CCI-002009The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.NIST SP 800-53 Revision 4 :: IA-8 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records containing the full-text recording of privileged commands or the individual identities of group account users.
STIG ID: SRG-APP-000101 **Rule ID:** SV-204727r508029_rule **Vul ID:** V-204727
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployment configuration to determine if the application server is configured to generate full-text recording of privileged commands or the individual identities of group users at a minimum.

Have a user execute a privileged command and review the log data to validate that the full-text or identity of the individual is being logged.

If the application server is not meeting this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. Configure the log ingestion pipeline including Logstash/Beats to generate log records containing the full-text recording of privileged commands or the individual identities of group account users. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch Security Settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
m. Auditbeat: https://www.elastic.co/beats/auditbeat
n. Filebeat: https://www.elastic.co/beats/filebeat
o. Metricbeat: https://www.elastic.co/beats/metricbeat
p. Packetbeat: https://www.elastic.co/beats/packetbeat
q. Heartbeat: https://www.elastic.co/beats/heartbeat
r. Winlogbeat: https://www.elastic.co/beats/winlogbeat
s. Logstash: https://www.elastic.co/logstash
t. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
u. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
v. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Privileged commands are commands that change the configuration or data of the application server. Since this type of command changes the application server configuration and could possibly change the security posture of the application server, these commands need to be logged to show the full-text of the command executed. Without the full-text, reconstruction of harmful events or forensic analysis is not possible.

Organizations can consider limiting the additional log information to only that information explicitly needed for specific log requirements. At a minimum, the organization must log

either full-text recording of privileged commands or the individual identities of group users, or both. The organization must maintain log trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Legacy Ids: V-57417; SV-71689

Comments:

CCI: CCI-000135The information system generates audit records containing the organization-defined additional more detailed information that is to be included in the audit records.NIST SP 800-53 :: AU-3 (1)NIST SP 800-53A :: AU-3 (1).1 (ii)NIST SP 800-53 Revision 4 :: AU-3 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.
STIG ID: SRG-APP-000403 **Rule ID:** SV-204807r508029_rule **Vul ID:** V-204807
Severity: CAT II

Documentable: No

Check Content:
The CAC is the standard DoD authentication token;the PIV is the standard authentication token used by federal/civilian agencies.

If access to the application server is limited to DoD personnel accessing the system via CAC; and PIV access is not warranted or allowed as per the system security plan, the PIV requirement is NA.

Review the application server documentation and configuration to determine if the application server electronically verifies PIV credentials from other federal agencies to access the management interface.

If the application server does not electronically verify other federal agency PIV credentials to access the management interface, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. PIV credentials are only used in an unclassified environment.

If PIV credentials are not electronically verified before accessing the management interface, unauthorized users may gain access to the system and data the user has not been granted access to.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57517; SV-71793

Comments:

CCI: CCI-002010The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.NIST SP 800-53 Revision 4 :: IA-8 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must alert the SA and ISSO, at a minimum, in the event of a log processing failure.
STIG ID: SRG-APP-000108 **Rule ID:** SV-204728r508029_rule **Vul ID:** V-204728
Severity: CAT II

Documentable: No

Check Content:
Review application server log configuration. Verify the application server sends alerts to the SA and ISSO in the event of a log processing failure.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

Recommend establishing an alert for SA and ISSO, at a minimum, that triggers in the event of a log processing failure.

1. The Elastic Stack API can be used to setup alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Kibana Alerts
The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify you of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. However, they can be tailored to meet the organization needs.

Missing monitoring data:
This alert is triggered when any stack product nodes or instances stop sending monitoring data. By default, the trigger condition is set to missing for 15 minutes looking back 1 day. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 6 hours.

References:

a. How monitoring works:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/how-monitoring-works.html
b. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
c. Kibana Alerts: https://www.elastic.co/guide/en/kibana/8.0/kibana-alerts.html
d. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/collecting-monitoring-data.html
e. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
f. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
g. cat nodes API: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-nodes.html
h. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Logs are essential to monitor the health of the system, investigate changes that occurred to the system, or investigate a security incident. When log processing fails, the events during the failure can be lost. To minimize the timeframe of the log failure, an alert needs to be sent to the SA and ISSO at a minimum.

Log processing failures include, but are not limited to, failures in the application server log capturing mechanisms or log storage capacity being reached or exceeded. In some instances, it is preferred to send alarms to individuals rather than to an entire group. Application servers must be able to trigger an alarm and send an alert to, at a minimum, the SA and ISSO in the event there is an application server log processing failure.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35186; SV-46473

Comments:

CCI: CCI-000139The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.NIST SP 800-53 :: AU-5 aNIST SP 800-53A :: AU-5.1 (ii)NIST SP 800-53 Revision 4 :: AU-5 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must accept FICAM-approved third-party credentials.
STIG ID: SRG-APP-000404 **Rule ID:** SV-204808r508029_rule **Vul ID:** V-204808
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server accepts FICAM-approved third-party credentials.

If the application server does not accept FICAM-approved third-party credentials, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

2. The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users. When using an IdP, Elasticsearch supports Federal Identity, Credential, and Access Management (FICAM) issued profiles such as SAML 2.0 and OpenID 2.0.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

i. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
j. Federal Identity, Credential, and Access Management Architecture:
https://arch.idmanagement.gov/
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Access may be denied to legitimate users if FICAM-approved third-party credentials are not accepted.

This requirement typically applies to organizational information systems that are accessible to non-federal government agencies and other partners. This allows federal government relying parties to trust such credentials at their approved assurance levels.

Third-party credentials are those credentials issued by non-federal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57519; SV-71795

Comments:

CCI: CCI-002011The information system accepts FICAM-approved third-party credentials.NIST SP 800-53 Revision 4 :: IA-8 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must shut down by default upon log failure (unless availability is an overriding concern).
STIG ID: SRG-APP-000109 **Rule ID:** SV-204729r508029_rule **Vul ID:** V-204729
Severity: CAT II

Documentable: No

Check Content:
If the application server is a high availability system, this finding is NA.

Review the application server configuration settings to determine if the application server is configured to shut down on a log failure.

If the application server is not configured to shut down on a log failure, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch will go into a read-only state when it detects issues with disk storage which is the most common issue affecting logging. Elasticsearch will not shutdown if logging fails for other reasons.

Elasticsearch should be configured so as to continue to log but cache the logs locally until log shipment can resume. Capacity of the disk receiving logs is generally the issue that causes this sort of failure. Availability is generally an overriding concern, so rather than shutting down when the log shipping fails, local caching should be used to keep the system available and permit "catching up" on log shipment once the issue is resolved. Per NIST 800-53, it is preferable to overwrite logs rather than shut down logging if there is no other option. Also recommend establishing an alert that triggers when logs fail to ship after collection for any reason, so the issue can be detected and resolved in a timely manner, before overwriting must be used as a measure of last resort to keep the system available.

2. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Returns information about a cluster’s nodes.
Request
GET /_cat/nodes

disk.total, dt, diskTotal
Total disk space, such as 458.3gb.
disk.used, du, diskUsed
Used disk space, such as 259.8gb.
disk.avail, d, disk, diskAvail
Available disk space, such as 198.4gb.
disk.used_percent, dup, diskUsedPercent
Used disk space percentage, such as 47.

3. Kibana Alerts: The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify you of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. However, you can tailor them to meet your specific needs.

Missing monitoring data:
This alert is triggered when any stack products nodes or instances stop sending monitoring data. By default, the trigger condition is set to missing for 15 minutes looking back 1 day. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 6 hours.

Disk usage threshold:
This alert is triggered when a node is nearly at disk capacity. By default, the trigger condition is set at 80% or more averaged over the last 5 minutes. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 1 day.

References:

a. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/how-monitoring-works.html
b. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
c. Kibana Alerts: https://www.elastic.co/guide/en/kibana/8.0/kibana-alerts.html
d. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/collecting-monitoring-data.html
e. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
f. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
g. cat nodes API: https:/hwww.elastic.co/guide/en/elasticsearch/reference/8.0/cat-nodes.html
h. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical that, when a system is at risk of failing to process logs, it detects and takes action to mitigate the failure. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. During a failure, the application server must be configured to shut down unless the application server is part of a high availability system.

When availability is an overriding concern, other approved actions in response to a log failure are as follows:

(i) If the failure was caused by the lack of log record storage capacity, the application must continue generating log records if possible (automatically restarting the log service if necessary), overwriting the oldest log records in a first-in-first-out manner.

(ii) If log records are sent to a centralized collection server and communication with this server is lost or the server fails, the application must queue log records locally until communication is restored or until the log records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local log data with the collection server.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35190; SV-46477

Comments:

CCI: CCI-000140The information system takes organization-defined actions upon audit failure (e.g.shut down information system, overwrite oldest audit records stop generating audit records).NIST SP 800-53 :: AU-5 bNIST SP 800-53A :: AU-5.1 (iv)NIST SP 800-53 Revision 4 :: AU-5 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must conform to FICAM-issued profiles.
STIG ID: SRG-APP-000405 **Rule ID:** SV-204809r508029_rule **Vul ID:** V-204809
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server conforms to FICAM-issued profiles.

If the application server does not conform to FICAM-issued profiles, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

2. The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users. When using an IdP, Elasticsearch supports Federal Identity, Credential, and Access Management (FICAM) issued profiles such as SAML 2.0 and OpenID 2.0.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
j. Federal Identity, Credential, and Access Management Architecture:
https://arch.idmanagement.gov/
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without conforming to FICAM-issued profiles, the information system may not be interoperable with FICAM-authentication protocols, such as SAML 2.0 and OpenID 2.0.

This requirement addresses open identity management standards.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57521; SV-71797

Comments:

CCI: CCI-002014The information system conforms to FICAM-issued profiles.NIST SP 800-53 Revision 4 :: IA-8 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured to fail over to another system in the event of log subsystem failure.
STIG ID: SRG-APP-000109 **Rule ID:** SV-204730r508029_rule **Vul ID:** V-204730
Severity: CAT II

Documentable: No

Check Content:
If the system MAC level and availability do not require redundancy, this requirement is NA.

Review the system's accreditation documentation to determine system MAC and confidentiality requirements. Review application server configuration settings to determine if the application server is configured to fail over operation to another system when the log subsystem fails to operate.

If the system MAC level requires redundancy and the application server is not configured to fail over to another system which can handle application and log functions when a log subsystem failure occurs, this is a finding.

Fix Text:
Steps/Recommendation:

If the system MAC level and availability do not require redundancy, this requirement is NA.

1. Elasticsearch provides a clustering capability by design and can be configured in a high-availability (HA) cluster. Elasticsearch offers a number of features to achieve HA despite failures.

- With proper planning, a cluster can be designed for resilience to many of the things that commonly go wrong, from the loss of a single node or network connection right up to a zone-wide outage such as power loss.
- Enable cross-cluster replication to replicate data to a remote follower cluster which may be in a different data centre or even on a different continent from the leader cluster. The follower cluster acts as a hot standby, ready to fail over in the event of a disaster so severe that the leader cluster fails. The follower cluster can also act as a geo-replica to serve searches from nearby clients.
- The last line of defense against data loss is to take regular snapshots of the cluster so that a copy can be restored elsewhere if needed.

Designing for resilience
A resilient cluster requires redundancy for every required cluster component. This means a resilient cluster must have:
- At least three master-eligible nodes
- At least two nodes of each role
- At least two copies of each shard (one primary and one or more replicas)

Back up a cluster:
WARNING: An Elasticsearch cluster cannot be backed up simply by copying the data directories of all of its nodes. Elasticsearch may be making changes to the contents of its data directories while it is running; copying its data directories cannot be expected to capture a consistent picture of their contents. If restoring a cluster from such a backup, it may fail and report corruption and/or missing files. Alternatively, it may appear to have succeeded though it silently lost some of its data. The only reliable way to back up a cluster is by using the snapshot and restore functionality.

To have a complete backup for a cluster:
- Back up the data
- Back up the cluster configuration
- Back up the security configuration

2. If using Elasticsearch as a SaaS product (Elastic-hosted), recommend a minimum of three availability zones to enable Elastic Cloud Enterprise to create clusters with a tiebreaker.

High availability
- Fault tolerance for Elastic Cloud Enterprise is based around the concept of availability zones.
- An availability zone contains resources available to an Elastic Cloud Enterprise installation that are isolated from other availability zones to safeguard against potential failure.
- If there are only two availability zones in total in the installation, no tiebreaker is created.

3. Refer to the cloud provider options of Regions and Availability Zones for high-availability (HA) cluster for hosting the Elastic cluster.

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html
c. Set up a cluster for high availability:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability.html
d. Designing for resilience:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability-cluster-design.html
e. Cross-cluster replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html
f. Back up a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/backup-cluster.html
g. High availability: https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-ha.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This requirement is dependent upon system MAC and availability. If the system MAC and availability do not specify redundancy requirements, this requirement is NA.

It is critical that, when a system is at risk of failing to process logs as required, it detects and takes action to mitigate the failure.

Application servers must be capable of failing over to another system which can handle application and logging functions upon detection of an application log processing failure. This will allow continual operation of the application and logging functions while minimizing the loss of operation for the users and loss of log data.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35191; SV-46478

Comments:

CCI: CCI-000140The information system takes organization-defined actions upon audit failure (e.g. shut down information system, overwrite oldest audit records, stop generating audit records).NIST SP 800-53 :: AU-5 bNIST SP 800-53A :: AU-5.1 (iv)NIST SP 800-53

Revision 4 :: AU-5 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions.
STIG ID: SRG-APP-000427 **Rule ID:** SV-204811r508029_rule **Vul ID:** V-204811
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server only allows the use of DoD PKI-established certificate authorities.

If the application server allows other certificate authorities for verification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
q. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates. The application server must only allow the use of DoD PKI-established certificate authorities for verification.

Legacy Ids: V-57551; SV-71827

Comments:

CCI: CCI-002470The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.NIST SP 800-53 Revision 4 :: SC-23 (5)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use internal system clocks to generate time stamps for log records.
STIG ID: SRG-APP-000116 **Rule ID:** SV-204731r508029_rule **Vul ID:** V-204731
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration files to determine if the internal system clock is used for time stamps. If this is not feasible, an alternative workaround is to take an action that generates an entry in the logs and then immediately query the operating system for the current time. A reasonable match between the two times will suffice as evidence that the system is using the internal clock for timestamps.

If the application server does not use the internal system clock to generate time stamps, this is a finding.

Fix Text:
Steps/Recommendation:

1. All applications should capture the time of log/event creation.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Recommended to setup NTP or Chrony in all host to avoid time drift in servers.

4. To verify if the ingest pipeline is setup to capture the time, use the following: GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. Processors:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest-processors.html
b. Ingest Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html
c. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/date-processor.html
d. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/get-pipeline-api.html
e. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
f. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
g. Install Elastic Agents:
https://www.elastic.co/guide/en/fleet/8.0/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without the use of an approved and synchronized time source configured on the systems, events cannot be accurately correlated and analyzed to determine what is transpiring within the application server.

If an event has been triggered on the network, and the application server is not configured with the correct time, the event may be seen as insignificant, when in reality the events are related and may have a larger impact across the network. Synchronization of system clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. Determining the correct time a particular event occurred on a system, via time stamps, is critical when conducting forensic analysis and investigating system events.

Application servers must utilize the internal system clock when generating time stamps and log records.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35203; SV-46490

Comments:

CCI: CCI-000159The information system uses internal system clocks to generate time stamps for audit records.NIST SP 800-53 :: AU-8NIST SP 800-53A :: AU-8.1NIST SP 800-53 Revision 4 :: AU-8 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.
STIG ID: SRG-APP-000428 **Rule ID:** SV-204812r508029_rule **Vul ID:** V-204812
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application

server implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.

If the application server does not implement cryptographic mechanisms to prevent unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an application server. Alternative physical protection measures include protected distribution systems.

In order to prevent unauthorized disclosure or modification of the information, application servers must protect data at rest by using cryptographic mechanisms.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either

encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Legacy Ids: V-57557; SV-71833

Comments:

CCI: CCI-002475The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.NIST SP 800-53 Revision 4 :: SC-28 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application must implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.
STIG ID: SRG-APP-000429 **Rule ID:** SV-204813r508029_rule **Vul ID:** V-204813
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.

If the application server does not implement cryptographic mechanisms to prevent unauthorized disclosure, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an application server. Alternative physical protection measures include protected distribution systems.

In order to prevent unauthorized disclosure or modification of the information, application servers must protect data at rest by using cryptographic mechanisms.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57559; SV-71835

Comments:

CCI: CCI-002476The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.NIST SP 800-53 Revision 4 :: SC-28 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log information from any type of unauthorized read access.
STIG ID: SRG-APP-000118 **Rule ID:** SV-204732r508029_rule **Vul ID:** V-204732
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log features protect log information from unauthorized access.

Review file system settings to verify the application server sets secure file permissions on log files.

If the application server does not protect log information from unauthorized read access, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized access with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to Elasticsearch cluster with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If log data were to become compromised, then competent forensic analysis and

discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve. In addition, access to log records provides information an attacker could potentially use to his or her advantage.

Application servers contain admin interfaces that allow reading and manipulation of log records. Therefore, these interfaces should not allow unfettered access to those records. Application servers also write log data to log files which are stored on the OS, so appropriate file permissions must also be used to restrict access.

Log information includes all information (e.g., log records, log settings, transaction logs, and log reports) needed to successfully log information system activity. Application servers must protect log information from unauthorized read access.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35205; SV-46492

Comments:

CCI: CCI-000162The information system protects audit information from unauthorized access.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server, when a MAC I system, must be in a high-availability (HA) cluster.
STIG ID: SRG-APP-000435 **Rule ID:** SV-204814r508029_rule **Vul ID:** V-204814
Severity: CAT II

Documentable: No

Check Content:
If the application server is not a MAC I system, this requirement is NA.

Review the application server documentation and configuration to determine if the application server is part of an HA cluster.

If the application server is not part of an HA cluster, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch provides a clustering capability by design and can be configured in a high-availability (HA) cluster. Elasticsearch offers a number of features to achieve HA despite failures.

- With proper planning, a cluster can be designed for resilience to many of the things that commonly go wrong, from the loss of a single node or network connection right up to a zone-wide outage such as power loss.
- Enable cross-cluster replication to replicate data to a remote follower cluster which may be in a different data centre or even on a different continent from the leader cluster. The follower cluster acts as a hot standby, ready to fail over in the event of a disaster so severe that the leader cluster fails. The follower cluster can also act as a geo-replica to serve searches from nearby clients.
- The last line of defense against data loss is to take regular snapshots of the cluster so that a copy can be restored elsewhere if needed.

Designing for resilience
A resilient cluster requires redundancy for every required cluster component. This means a resilient cluster must have:
- At least three master-eligible nodes
- At least two nodes of each role
- At least two copies of each shard (one primary and one or more replicas)

Back up a cluster
WARNING: An Elasticsearch cluster cannot be backed up simply by copying the data directories of all of its nodes. Elasticsearch may be making changes to the contents of its data directories while it is running; copying its data directories cannot be expected to capture a consistent picture of their contents. If restoring a cluster from such a backup, it may fail and report corruption and/or missing files. Alternatively, it may appear to have succeeded though it silently lost some of its data. The only reliable way to back up a cluster is by using the snapshot and restore functionality.

To have a complete backup for a cluster:
- Back up the data
- Back up the cluster configuration
- Back up the security configuration

2. If using Elasticsearch as a SaaS product (Elastic-hosted), recommend a minimum of three availability zones to enable Elastic Cloud Enterprise to create clusters with a tiebreaker.

High availability
- Fault tolerance for Elastic Cloud Enterprise is based around the concept of availability zones.
- An availability zone contains resources available to an Elastic Cloud Enterprise installation

that are isolated from other availability zones to safeguard against potential failure.
- If there are only two availability zones in total in the installation, no tiebreaker is created.

3. Refer to the cloud provider options of Regions and Availability Zones for high-availability (HA) cluster for hosting the Elastic cluster.

References:

a. Add and remove nodes in a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/current/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-node.html
c. Set up a cluster for high availability:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability.html
d. Designing for resilience:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability-cluster-design.html
e. Cross-cluster replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html
f. Create a snapshot:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/snapshots-take-snapshot.html
g. High availability: https://www.elastic.co/guide/en/cloud-enterprise/current/ece-ha.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A MAC I system is a system that handles data vital to the organization's operational readiness or effectiveness of deployed or contingency forces. A MAC I system must maintain the highest level of integrity and availability. By HA clustering the application server, the hosted application and data are given a platform that is load-balanced and provided high-availability.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57531; SV-71807

Comments:

CCI: CCI-002385The information system protects against or limits the effects of

organization-defined types of denial of service attacks by employing organization-defined security safeguards.NIST SP 800-53 Revision 4 :: SC-5

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log information from unauthorized modification.
STIG ID: SRG-APP-000119 **Rule ID:** SV-204733r508029_rule **Vul ID:** V-204733
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log features protect log information from unauthorized modification.

Review file system settings to verify the application server sets secure file permissions on log files to prevent unauthorized modification.

If the application server does not protect log information from unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized modification with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:

https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If log data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve. In addition, access to log records provides information an attacker could potentially use to his or her advantage.

Application servers contain admin interfaces that allow reading and manipulation of log records. Therefore, these interfaces should not allow unfettered access to those records. Application servers also write log data to log files which are stored on the OS, so appropriate file permissions must also be used to restrict access.

Log information includes all information (e.g., log records, log settings, transaction logs and log reports) needed to successfully log information system activity. Application servers must protect log information from unauthorized modification.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35772; SV-47059

Comments:

CCI: CCI-000163The information system protects audit information from unauthorized modification.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect against or limit the effects of all types of Denial of Service (DoS) attacks by employing organization-defined security safeguards.
STIG ID: SRG-APP-000435 **Rule ID:** SV-204815r508029_rule **Vul ID:** V-204815

Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server can protect against or limit the effects of all types of Denial of Service (DoS) attacks by employing defined security safeguards.

If the application server cannot be configured to protect against or limit the effects of all types of DoS, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Stack does not have any built in Denial of Service (DoS) capability, therefore it is recommended to leverage a third-party Host Intrusion Detection System (HIDS) or Host Intrusion Prevention System (HIPS).

2. The HIDS or HIPS application should be installed, configured, and updated on each application server.

Note: A HIDS or HIPS application is a secondary line of defense behind the antivirus. The application will monitor all ports and the dynamic state of a development system. If the application detects irregularities on the system, it will block incoming traffic that may potentially compromise the development system that can lead to a DoS or data theft.

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity. To reduce the possibility or effect of a DoS, the application server must employ defined security safeguards. These safeguards will be determined by the placement of the application server and the type of applications being hosted within the application server framework.

There are many examples of technologies that exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the application opens at one time). Employing increased capacity and bandwidth, combined with

service redundancy or clustering, may reduce the susceptibility to some DoS attacks.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57529; SV-71805

Comments:

CCI: CCI-002385The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.NIST SP 800-53 Revision 4 :: SC-5

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log information from unauthorized deletion.
STIG ID: SRG-APP-000120 **Rule ID:** SV-204734r508029_rule **Vul ID:** V-204734
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log features protect log information from unauthorized deletion.

Review file system settings to verify the application server sets secure file permissions on log files to prevent unauthorized deletion.

If the application server does not protect log information from unauthorized deletion, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized deletion with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege

permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If log data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve.

Application servers contain admin interfaces that allow reading and manipulation of log records. Therefore, these interfaces should not allow for unfettered access to those records. Application servers also write log data to log files which are stored on the OS, so appropriate file permissions must also be used to restrict access.

Log information includes all information (e.g., log records, log settings, transaction logs, and log reports) needed to successfully log information system activity. Application servers must protect log information from unauthorized deletion.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35212; SV-46499

Comments:

CCI: CCI-000164The information system protects audit information from unauthorized

deletion.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log tools from unauthorized access.
STIG ID: SRG-APP-000121 **Rule ID:** SV-204735r508029_rule **Vul ID:** V-204735
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and server configuration to determine if the application server protects log tools from unauthorized access.

Request a system administrator attempt to access log tools while logged into the server in a role that does not have the requisite privileges.

If the application server does not protect log tools from unauthorized access, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized access with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to Elasticsearch cluster with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting log data also includes identifying and protecting the tools used to view and manipulate log data.

Depending upon the log format and application, system and application log tools may provide the only means to manipulate and manage application and system log data.

It is, therefore, imperative that access to log tools be controlled and protected from unauthorized access.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected as well.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35213; SV-46500

Comments:

CCI: CCI-001493The information system protects audit tools from unauthorized access.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect the confidentiality and integrity of transmitted information through the use of an approved TLS version.
STIG ID: SRG-APP-000439 **Rule ID:** SV-204816r508029_rule **Vul ID:** V-204816
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine which version of TLS is being used.

If the application server is not using TLS to maintain the confidentiality and integrity of transmitted information or non-FIPS-approved SSL versions are enabled, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: Preventing the disclosure of transmitted information requires that the application server take measures to employ some form of cryptographic mechanism in order to protect the information during transmission. This is usually achieved through the use of Transport Layer Security (TLS).

Transmission of data can take place between the application server and a large number of devices/applications external to the application server. Examples are a web client used by a user, a backend database, a log server, or other application servers in an application server cluster.

If data is transmitted unencrypted, the data then becomes vulnerable to disclosure. The disclosure may reveal user identifier/password combinations, website code revealing business logic, or other user personal information.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-57533; SV-71809

Comments:

CCI: CCI-002418The information system protects the confidentiality and/or integrity of transmitted information.NIST SP 800-53 Revision 4 :: SC-8

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log tools from unauthorized modification.
STIG ID: SRG-APP-000122 **Rule ID:** SV-204736r508029_rule **Vul ID:** V-204736
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and server configuration to determine if the application server protects log tools from unauthorized modification. Request a system administrator attempt to modify log tools while logged into the server in a role that does not have the requisite privileges.

Locate binary copies of log tool executables that are located on the file system and attempt to modify using unprivileged credentials.

If the application server does not protect log tools from unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized modification with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting log data also includes identifying and protecting the tools used to view and manipulate log data.

Depending upon the log format and application, system and application log tools may provide the only means to manipulate and manage application and system log data.

It is, therefore, imperative that access to log tools be controlled and protected from unauthorized modification. If an attacker were to modify log tools, he could also manipulate logs to hide evidence of malicious activity.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected as well.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35214; SV-46501

Comments:

CCI: CCI-001494The information system protects audit tools from unauthorized modification.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must remove all export ciphers to protect the confidentiality and integrity of transmitted information.
STIG ID: SRG-APP-000439 **Rule ID:** SV-204817r508029_rule **Vul ID:** V-204817
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine if export ciphers are removed.

If the application server does not have the export ciphers removed, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html

k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: During the initial setup of a Transport Layer Security (TLS) connection to the application server, the client sends a list of supported cipher suites in order of preference. The application server will reply with the cipher suite it will use for communication from the client list. If an attacker can intercept the submission of cipher suites to the application server and place, as the preferred cipher suite, a weak export suite, the encryption used for the session becomes easy for the attacker to break, often within minutes to hours.

Legacy Ids: V-61351; SV-75833

Comments:

CCI: CCI-002418The information system protects the confidentiality and/or integrity of transmitted information.NIST SP 800-53 Revision 4 :: SC-8

Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect log tools from unauthorized deletion.
STIG ID: SRG-APP-000123 **Rule ID:** SV-204737r508029_rule **Vul ID:** V-204737
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and server configuration to determine if the application server protects log tools from unauthorized deletion.

Locate binary copies of log tool executables that are located on the file system and attempt to delete using unprivileged credentials.

If the application server does not protect log tools from unauthorized deletion, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Enabling security protects Elasticsearch clusters by preventing unauthorized deletion with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes.

References:

a. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting log data also includes identifying and protecting the tools used to view and manipulate log data.

Depending upon the log format and application, system and application log tools may provide the only means to manipulate and manage application and system log data.

It is, therefore, imperative that access to log tools be controlled and protected from unauthorized modification. If an attacker were to delete log tools, the application server administrator would have no way of managing or viewing the logs.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar, class or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected from unauthorized deletion as well.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35215; SV-46502

Comments:

CCI: CCI-001495The information system protects audit tools from unauthorized deletion.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must employ approved cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.
STIG ID: SRG-APP-000440 **Rule ID:** SV-204818r508029_rule **Vul ID:** V-204818
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server employs approved cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

If the application server does not employ approved cryptographic mechanisms, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Preventing the disclosure or modification of transmitted information requires that application servers take measures to employ approved cryptography in order to protect the information during transmission over the network. This is usually achieved through the use of Transport Layer Security (TLS), SSL VPN, or IPSec tunnel.

If data in transit is unencrypted, it is vulnerable to disclosure and modification. If approved cryptographic algorithms are not used, encryption strength cannot be assured.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-57535; SV-71811

Comments:

CCI: CCI-002421The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards.NIST SP 800-53 Revision 4 :: SC-8 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must back up log records at least every seven days onto a different system or system component than the system or component being logged.
STIG ID: SRG-APP-000125 **Rule ID:** SV-204738r508029_rule **Vul ID:** V-204738
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server backs up log records every seven days onto a different system or media from the system being logged.

If the application server does not back up log records every seven days onto a different system or media from the system being logged, this is a finding.

Fix Text:
Steps/Recommendation:

1. Setup appropriate lifecycle for the indices and create snapshots.

2. Elasticsearch can be configured to provide redundancy by storing the Elasticsearch data into a different system or system component than the system or component being logged.

References:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/8.0/resiliency.html
b. Manage the index lifecycle:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-lifecycle-management.html
c. Configure snapshot lifecycle policies:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/getting-started-snapshot-lifecycle-management.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protection of log data includes assuring log data is not accidentally lost or deleted. Backing up log records to a different system or onto separate media from the system the application server is actually running on helps to assure that in the event of a catastrophic system failure, the log records will be retained.

Legacy Ids: V-35216; SV-46503

Comments:

CCI: CCI-001348The information system backs up audit records on an organization-defined frequency onto a different system or system component than the system or component being audited.NIST SP 800-53 :: AU-9 (2)NIST SP 800-53A :: AU-9 (2).1 (iii)NIST SP 800-53 Revision 4 :: AU-9 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must maintain the confidentiality and integrity of information during preparation for transmission.
STIG ID: SRG-APP-000441 **Rule ID:** SV-204819r508029_rule **Vul ID:** V-204819
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine if the

application server maintains the confidentiality and integrity of information during preparation before transmission.

If the confidentiality and integrity is not maintained, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:

https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

An example of this would be an SMTP queue. This queue may be part of the application server so error messages from the server can be sent to system administrators, or SMTP functionality can be added to hosted applications by developers.

Any modules used by the application server that queue data before transmission must maintain the confidentiality and integrity of the information before the data is transmitted.

Legacy Ids: V-57537; SV-71813

Comments:

CCI: CCI-002420The information system maintains the confidentiality and/or integrity of information during preparation for transmission.NIST SP 800-53 Revision 4 :: SC-8 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use cryptographic mechanisms to protect the integrity of log information.
STIG ID: SRG-APP-000126 **Rule ID:** SV-204739r508029_rule **Vul ID:** V-204739
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server can be configured to protect the integrity of log data using cryptographic hashes and digital signatures. Configure the application server to hash and sign log data. This is typically done the moment when log files cease to be written to and are rolled over for storage or offloading.

Alternatively, if the application server is not able to hash and sign log data, the task can be delegated by configuring the application server or underlying OS to send logs to a centralized log management system or SIEM that can meet the requirement.

If the application server is not configured to hash and sign logs, or is not configured to utilize the aforementioned OS and centralized log management resources to meet the requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. For the Elastic cloud hosted service offerings, Elastic uses Auditbeat and Elastic Endpoint

Security as host-based intrusion detection system and File Integrity Management (HIDS)/(FIM) on all hosts, specifying files and directories to be monitored for changes. File changes are detected in near real time and sent to Elasticsearch clusters in the Security Control Plane with metadata and cryptographic hashes of the file to enable further analysis. If unauthorized changes or anomalous connections are detected in the AWS infrastructure, an alert is generated from the Elasticsearch clusters to notify the Information Security team of an anomalous event.

2. For an on-premise Elasticsearch deployment, it is recommended that a third party HIDS/FIM be implemented as a risk reduction method for this control.

References:

a. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
b. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting the integrity of log records helps to ensure log files are not tampered with. Cryptographic mechanisms are the industry-established standard used to protect the integrity of log data. An example of cryptographic mechanisms is the computation and application of a cryptographic hash and using asymmetric cryptography with digital signatures. Application Servers often write log data to files on the file system. These files typically roll over on a periodic basis. Once the logs are rolled over, hashing and signing the logs assures the logs are not tampered with and helps to assure log integrity.

Legacy Ids: V-35217; SV-46504

Comments:

CCI: CCI-001350The information system implements cryptographic mechanisms to protect the integrity of audit information.NIST SP 800-53 :: AU-9 (3)NIST SP 800-53A :: AU-9 (3).1NIST SP 800-53 Revision 4 :: AU-9 (3)

Rule Title: The application server must maintain the confidentiality and integrity of information during reception.
STIG ID: SRG-APP-000442 **Rule ID:** SV-204820r508029_rule **Vul ID:** V-204820
Severity: CAT II

Documentable: No

Check Content:
Review application server configuration to determine if the server is using a transmission method that maintains the confidentiality and integrity of information during reception.

If a transmission method is not being used that maintains the confidentiality and integrity of the data during reception, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the Elasticsearch to maintain the confidentiality and integrity of information during preparation for transmission by configuring SSL/TLS encryption as well as encryption at rest of data stored in the Elastic cluster.

1. Enable Authentication and Authorization

2. Enable SSL/TLS encryption

3. Enable IP filtering

4. Disable anonymous user access to Elasticsearch if enabled.

Note: Incoming requests are considered to be anonymous if no authentication token can be extracted from the incoming request. By default, anonymous requests are rejected and an authentication error is returned (status code 401).

5. In elasticsearch.yml set
xpack.security.enabled: true
xpack.security.fips_mode.enabled: true

To enable encryption, you need to perform the following steps on each node in the cluster:

a. Generate a private key and X.509 certificate for each of your Elasticsearch nodes. See Generating Node Certificates.
b. Configure each node in the cluster to identify itself using its signed certificate and enable TLS on the transport layer. You can also optionally enable TLS on the HTTP layer. See Encrypting communications between nodes in a cluster and Encrypting HTTP client communications.

c. Configure the monitoring features to use encrypted connections. See Monitoring and security.
d. Configure Kibana to encrypt communications between the browser and the Kibana server and to connect to Elasticsearch via HTTPS. See Configuring security in Kibana.
e. Configure Logstash to use TLS encryption. See Configuring security in Logstash.
f. Configure Beats to use encrypted connections. For example, see Configure Filebeat to use security features.
g. Configure the Java transport client to use encrypted communications. See Java Client and security.
h. Configure Elasticsearch for Apache Hadoop to use secured transport. See Elasticsearch for Apache Hadoop Security.

6. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers with Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography).

7. Elastic Cloud Enterprise does not implement encryption at rest out of the box. To ensure encryption at rest for all data managed by Elastic Cloud Enterprise, the hosts running Elastic Cloud Enterprise must be configured with disk-level encryption, such as dm-crypt. In addition, snapshot targets must ensure that data is encrypted at rest as well.

8. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

References:

a. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html
b. Encrypting communications in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
c. Setting Up TLS on a Cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ssl-tls.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. Configuring kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Working with certificates:
https://www.elastic.co/guide/en/elasticsearch/client/net-api/8.0/working-with-certificates.html
p. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
q. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/current/ece-securing-considerations.html
r. Support Matrix: https://www.elastic.co/support/matrix
s. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information can be either unintentionally or maliciously disclosed or modified during reception, including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Protecting the confidentiality and integrity of received information requires that application servers take measures to employ approved cryptography in order to protect the information during transmission over the network. This is usually achieved through the use of Transport Layer Security (TLS), SSL VPN, or IPSEC tunnel.

The application server must utilize approved encryption when receiving transmitted data.

Legacy Ids: V-57539; SV-71815

Comments:

CCI: CCI-002422The information system maintains the confidentiality and/or integrity of information during reception.NIST SP 800-53 Revision 4 :: SC-8 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.
STIG ID: SRG-APP-000131 **Rule ID:** SV-204740r508029_rule **Vul ID:** V-204740
Severity: CAT II

Documentable: No

Check Content:
Review system documentation to determine if the application server prevents the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, the Elasticsearch system does not prevent the installation of patches, service packs, or application components without verifying the software component has been digitally signed using a certificate that is recognized and approved by the organization.

Configure the operating system to verify the signature of local packages prior to install with a certificate recognized and approved by an organizationally maintained certificate authority.

2. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to verify the signature of packages prior to install of patches, service packs, or application components with a certificate recognized and approved by the an organizationally maintained certificate authority. Self-signed certificates are disallowed by this requirement.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Changes to any software components can have significant effects on the overall security of the application. Verifying software components have been digitally signed using a certificate that is recognized and approved by the organization ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, or application components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The application should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Legacy Ids: V-57495; SV-71771

Comments:

CCI: CCI-001749The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.NIST SP 800-53 Revision 4 :: CM-5 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.
STIG ID: SRG-APP-000447 **Rule ID:** SV-204821r508029_rule **Vul ID:** V-204821
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the management interface behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommended using the Kibana UI to manage the Elastic Stack and that Kibana performs input validation checks. Access to individual features is governed by Elasticsearch and Kibana privileges.

References:

a. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html
b. Security best practices:
https://www.elastic.co/guide/en/kibana/8.0/security-best-practices.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Invalid user input occurs when a user inserts data or characters into an applications data entry field and the application is unprepared to process that data. This results in unanticipated application behavior potentially leading to an application or information system compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

Application servers must ensure their management interfaces perform data input validation checks. When invalid data is entered, the application server must behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received. An example of a predictable behavior is trapping the data, logging the invalid data for forensic analysis if necessary, and continuing operation in a safe and secure manner.

Legacy Ids: V-57565; SV-71841

Comments:

CCI: CCI-002754The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.NIST SP 800-53 Revision 4 :: SI-10 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must limit privileges to change the software resident within software libraries.
STIG ID: SRG-APP-000133 **Rule ID:** SV-204741r508029_rule **Vul ID:** V-204741
Severity: CAT II

Documentable: No

Check Content:
Check the application server documentation and configuration to determine if the application server provides role-based access that limits the capability to change shared software libraries.

Validate file permission settings to ensure library files are secured in relation to OS access.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1.For on premises implementation, the Elasticsearch system does not prevent modifications on the software resident within software libraries.

Configure the application OS file permissions to restrict access to software libraries and configure the application to restrict user access regarding software library update functionality to only authorized users or processes. For example, the Elasticsearch directory contents include among others:
LICENSE.txt, NOTICE.txt, README.asciidoc, bin, config, data, jdk, lib, logs, modules, plugins

Recommend establishing an alert for detecting such system changes so they can be evaluated promptly. For the hosted Elasticsearch Service (SaaS offering), only an Elastic Admin with access to the Infrastructure as Code files would be able to modify files and modules that cannot be configured directly by Customer. Customer is responsible for secure configuration with Role-based access control (RBAC) controls. Elastic monitors for such changes in the hosted production environment and investigates if detected.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers have the ability to specify that the hosted applications utilize shared libraries. The application server must have a capability to divide roles based upon duties wherein one project user (such as a developer) cannot modify the shared library code of another project user. The application server must also be able to specify that non-privileged users cannot modify any shared library code at all.

Legacy Ids: V-35224; SV-46511

Comments:

CCI: CCI-001499The organization limits privileges to change software resident within software libraries.NIST SP 800-53 :: CM-5 (6)NIST SP 800-53A :: CM-5 (6).1NIST SP 800-53 Revision 4 :: CM-5 (6)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must remove organization-defined software components after updated versions have been installed.
STIG ID: SRG-APP-000454 **Rule ID:** SV-204822r508029_rule **Vul ID:** V-204822
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if organization-defined software components are removed after updated versions have been installed.

If organization-defined software components are not removed after updated versions have been installed, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, review all the nodes of the cluster to remove organization-defined software components after updated versions have been installed.

2. As part of the hosted Elasticsearch Service offering, review all the nodes of the cluster to

remove organization-defined software components after updated versions have been installed.

ECE supports rolling upgrades on an Elasticsearch cluster to be upgraded one node at a time so upgrading does not interrupt service.

3. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to remove organization-defined software components after updated versions have been installed.

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Rolling upgrades:
https://www.elastic.co/guide/en/elasticsearch/reference/current/rolling-upgrades.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Installation of patches and updates is performed when there are errors or security vulnerabilities in the current release of the software. When previous versions of software components are not removed from the application server after updates have been installed, an attacker may use the older components to exploit the system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57563; SV-71839

Comments:

CCI: CCI-002617The organization removes organization-defined software components (e.g. previous versions) after updated versions have been installed.NIST SP 800-53 Revision 4 :: SI-2 (6)

Rule Title: The application server must be capable of reverting to the last known good configuration in the event of failed installations and upgrades.
STIG ID: SRG-APP-000133 **Rule ID:** SV-204742r508029_rule **Vul ID:** V-204742
Severity: CAT II

Documentable: No

Check Content:
Check the application server documentation and configuration to determine if the application server provides an automated rollback capability to a known good configuration in the event of a failed installation and upgrade.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. As part of the hosted Elasticsearch Service offering, customers may configure how they wish to run backups to enable rollback or restore of their configurations. Elastic is responsible for SaaS and system wide capabilities for snapshot and restore operations at the SaaS layer level. Use of ECE, ECK, or Elastic Cloud is recommended; rollback is not supported by Elastic for "self-managed" implementations.

ECE supports rolling upgrades on an Elasticsearch cluster to be upgraded one node at a time so upgrading does not interrupt service.

2. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to enable rollback or restore to the last known good configuration in the event of failed installations and upgrades.

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Rolling upgrades:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/rolling-upgrades.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Any changes to the components of the application server can have significant effects on the overall security of the system.

In order to ensure a prompt response to failed application installations and application server upgrades, the application server must provide an automated rollback capability that allows the system to be restored to a previous known good configuration state prior to the application installation or application server upgrade.

Legacy Ids: V-57497; SV-71773

Comments:

CCI: CCI-001499The organization limits privileges to change software resident within software libraries.NIST SP 800-53 :: CM-5 (6)NIST SP 800-53A :: CM-5 (6).1NIST SP 800-53 Revision 4 :: CM-5 (6)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must install security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).
STIG ID: SRG-APP-000456 **Rule ID:** SV-204823r508029_rule **Vul ID:** V-204823
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server checks with a patch management system to install security-relevant software updates within a timeframe directed by an authoritative source.

If the application server does not install security-relevant patches within the time period directed by the authoritative source, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, review all the nodes of the cluster to install security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

2. As part of the hosted Elasticsearch Service offering, Elastic Cloud installs security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

3. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to install security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Release notes:
https://www.elastic.co/guide/en/elasticsearch/reference/current/es-release-notes.html
c. STIGs: https://cyber.mil/stigs/
d. NSA Configuration Guides:
https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/
e. CTOs: https://www.cybercom.mil/
f. DTMs: https://www.esd.whs.mil/DD/DoD-Issuances/DTM/

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes) to production systems after thorough testing of the patches within a lab environment. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57561; SV-71837

Comments:

CCI: CCI-002605The organization installs security-relevant software updates within organization-defined time period of the release of the updatesNIST SP 800-53 Revision 4 :: SI-2 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must adhere to the principles of least functionality by providing only essential capabilities.
STIG ID: SRG-APP-000141 **Rule ID:** SV-204743r508029_rule **Vul ID:** V-204743
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server can disable non-essential features and capabilities.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. All audit logging requirements can be configured in elasticsearch.yml. The audit requirement should be defined by the line of business in the system security plan document. The configuration should match all the required audit attributes defined in the system security plan document.

2. To enable the required attributes as defined in the document, refer to latest documentation for full set of supported attributes:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

3. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts which need to be secured to match all the required audit attributes defined in the system security plan document.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html

f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers provide a myriad of differing processes, features and functionalities. Some of these processes may be deemed to be unnecessary or too unsecure to run on a production DoD system. Application servers must provide the capability to disable or deactivate functionality and services that are deemed to be non-essential to the server mission or can adversely impact server performance, for example, disabling dynamic JSP reloading on production application servers as a best practice.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35234; SV-46521

Comments:

CCI: CCI-000381The organization configures the information system to provide only essential capabilities.NIST SP 800-53 :: CM-7NIST SP 800-53A :: CM-7.1 (ii)NIST SP 800-53 Revision 4 :: CM-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful attempts to modify privileges occur.
STIG ID: SRG-APP-000495 **Rule ID:** SV-204824r508029_rule **Vul ID:** V-204824

Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when successful/unsuccessful attempts are made to modify privileges.

If log records are not generated, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Changing privileges of a subject/object may cause a subject/object to gain or lose capabilities. When successful/unsuccessful changes are made, the event needs to be logged. By logging the event, the modification or attempted modification can be investigated to determine if it was performed inadvertently or maliciously.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57439; SV-71711

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prohibit or restrict the use of nonsecure ports, protocols, modules, and/or services as defined in the PPSM CAL and vulnerability assessments.
STIG ID: SRG-APP-000142 **Rule ID:** SV-204744r508029_rule **Vul ID:** V-204744
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployment configuration to determine which ports and protocols are enabled.

Verify that the ports and protocols being used are not prohibited and are necessary for the operation of the application server and the hosted applications.

If any of the ports or protocols is prohibited or not necessary for the application server operation, this is a finding.

Fix Text:
Steps/Recommendation:

1. Ensure all available ports are registered with PPSM.

2. Each Elasticsearch node has two different network interfaces. Clients send requests to Elasticsearch's REST APIs using its HTTP interface, but nodes communicate with other nodes using the transport interface. The transport interface is also used for communication with remote clusters.

The network settings described above apply to both methods of communication, and you can also configure each interface separately if needed.

3. The following settings can be configured for HTTP in elasticsearch.yml. By default, Elasticsearch runs on 9200 port. These settings also use the common network settings.

http.port
(Static) A bind port range. Defaults to 9200-9300.
http.publish_port
(Static) The port that HTTP clients should use when communicating with this node. Useful when a cluster node is behind a proxy or firewall and the http.port is not directly addressable from the outside. Defaults to the actual port assigned via http.port.
http.bind_host
(Static) The host address to bind the HTTP service to. Defaults to http.host (if set) or network.bind_host.
http.publish_host
(Static) The host address to publish for HTTP clients to connect to. Defaults to http.host (if set) or network.publish_host.
http.host
(Static) Used to set the http.bind_host and the http.publish_host.

4. The following settings can be configured for the internal transport that communicates over TCP in elasticsearch.yml.

The transport layer is used for all internal communication between nodes within a cluster, all

communication with the nodes of a remote cluster, and also by the TransportClient in the Elasticsearch Java API.

Transport settings
Some of the available settings are presented below for brevity.

transport.port
(Static) A bind port range. Defaults to 9300-9400.
transport.publish_port
(Static) The port that other nodes in the cluster should use when communicating with this node. Useful when a cluster node is behind a proxy or firewall and the transport.port is not directly addressable from the outside. Defaults to the actual port assigned via transport.port.
transport.bind_host
(Static) The host address to bind the transport service to. Defaults to transport.host (if set) or network.bind_host.
transport.publish_host
(Static) The host address to publish for nodes in the cluster to connect to. Defaults to transport.host (if set) or network.publish_host.
transport.host

References:

a. DoD ports and protocols PPSM web site: https://public.cyber.mil/connect/ppsm/
b. HTTP:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-http.html#_http_settings
c. Configuring Elasticsearch Transport:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-transport.html
d. Network settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-network.html
e. ECE Networking:
https://www.elastic.co/guide/en/cloud-enterprise/2.6/ece-prereqs-networking.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Some networking protocols may not meet organizational security requirements to protect data and components.

Application servers natively host a number of various features, such as management interfaces, httpd servers and message queues. These features all run on TCP/IP ports. This creates the potential that the vendor may choose to utilize port numbers or network services

that have been deemed unusable by the organization. The application server must have the capability to both reconfigure and disable the assigned ports without adversely impacting application server operation capabilities. For a list of approved ports and protocols, reference the DoD ports and protocols web site at https://public.cyber.mil/connect/ppsm/

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57501; SV-71777

Comments:

CCI: CCI-000382The organization configures the information system to prohibit or restrict the use of organization defined functions ports, protocols, and/or services.NIST SP 800-53 :: CM-7NIST SP 800-53A :: CM-7.1 (iii)NIST SP 800-53 Revision 4 :: CM-7 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful attempts to delete privileges occur.
STIG ID: SRG-APP-000499 **Rule ID:** SV-204825r508029_rule **Vul ID:** V-204825
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when successful and unsuccessful attempts are made to delete privileges.

If log records are not generated, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as

xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Deleting privileges of a subject/object may cause a subject/object to gain or lose capabilities. When successful and unsuccessful privilege deletions are made, the events need to be logged. By logging the event, the modification or attempted modification can be investigated to determine if it was performed inadvertently or maliciously.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57441; SV-71713

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use an enterprise user management system to uniquely identify and authenticate users (or processes acting on behalf of organizational users).
STIG ID: SRG-APP-000148 **Rule ID:** SV-204745r508029_rule **Vul ID:** V-204745
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server is using an enterprise solution to authenticate organizational users and processes running on the users' behalf.

If an enterprise solution is not being used, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with these services to uniquely identify and authenticate users (or processes acting on behalf of organizational users).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html

b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure accountability and prevent unauthorized access, application server users must be uniquely identified and authenticated. This is typically accomplished via the use of a user store which is either local (OS-based) or centralized (LDAP) in nature.

To ensure support to the enterprise, the authentication must utilize an enterprise solution.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35299; SV-46586

Comments:

CCI: CCI-000764The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).NIST SP 800-53 :: IA-2NIST SP 800-53A :: IA-2.1NIST SP 800-53 Revision 4 :: IA-2

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use multifactor authentication for network access to privileged accounts.
STIG ID: SRG-APP-000149 **Rule ID:** SV-204746r508029_rule **Vul ID:** V-204746
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to ensure the system is authenticating via multifactor authentication for privileged users.

If all aspects of application server web management interfaces are not authenticating privileged users via multifactor authentication methods, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using an external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm enforce to ensure the system is authenticating via multifactor authentication for privileged users.

2. On hosted Elasticsearch Service (SaaS offering), follow the steps to enable multi-factor authentication:
To enable multi-factor authentication, you must enroll your device.

- Log in to the Elasticsearch Service Console.
- Go to Settings.
- Click Configure to enable the Authenticator app or Add a phone number to enable the Text message.

References:

a. Enable multi-factor authentication:
https://www.elastic.co/guide/en/cloud/current/ec-account-user-settings.html#ec-account-security-mfa
b. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
d. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
e. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
f. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
g. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
h. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
i. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Multifactor authentication creates a layered defense and makes it more difficult for an unauthorized person to access the application server. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Unlike a simple username/password scenario where the attacker could gain access by knowing both the username and password without the user knowing his account was compromised, multifactor authentication adds the requirement that the attacker must have something from the user, such as a token, or to biometrically be the user.

Multifactor authentication is defined as: using two or more factors to achieve authentication.

Factors include:
(i) something a user knows (e.g., password/PIN);
(ii) something a user has (e.g., cryptographic identification device, token); or
(iii) something a user is (e.g., biometric). A CAC or PKI Hardware Token meets this definition.

A privileged account is defined as an information system account with authorizations of a privileged user. These accounts would be capable of accessing the web management interface.

When accessing the application server via a network connection, administrative access to the application server must be PKI Hardware Token enabled.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35300; SV-46587

Comments:

CCI: CCI-000765The information system implements multifactor authentication for network access to privileged accounts.NIST SP 800-53 :: IA-2 (1)NIST SP 800-53A :: IA-2 (1).1NIST SP 800-53 Revision 4 :: IA-2 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use multifactor authentication for local access to privileged accounts.
STIG ID: SRG-APP-000151 **Rule ID:** SV-204747r508029_rule **Vul ID:** V-204747
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to ensure the system is authenticating via multifactor authentication for privileged users.

If all aspects of application server command line management interfaces are not authenticating privileged users via multifactor authentication methods, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using an external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm enforce to ensure the system is authenticating via multifactor authentication for privileged users.

2. On hosted Elasticsearch Service (SaaS offering), follow the steps to enable multi-factor authentication:
To enable multi-factor authentication, you must enroll your device.
- Log in to the Elasticsearch Service Console.
- Go to Settings.
- Click Configure to enable the Authenticator app or Add a phone number to enable the Text message.

References:

a. Enable multi-factor authentication:

https://www.elastic.co/guide/en/cloud/current/ec-account-user-settings.html#ec-account-security-mfa
b. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
d. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
e. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
f. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
g. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
h. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
i. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Multifactor authentication creates a layered defense and makes it more difficult for an unauthorized person to access the application server. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Unlike a simple username/password scenario where the attacker could gain access by knowing both the username and password without the user knowing his account was compromised, multifactor authentication adds the requirement that the attacker must have something from the user, such as a token, or to biometrically be the user.

Multifactor authentication is defined as: using two or more factors to achieve authentication.

Factors include:
(i) something a user knows (e.g., password/PIN);
(ii) something a user has (e.g., cryptographic identification device, token); or
(iii) something a user is (e.g., biometric). A CAC or PKI Hardware Token meets this definition.

A privileged account is defined as an information system account with authorizations of a

privileged user. These accounts would be capable of accessing the command line management interface.

When accessing the application server via a network connection, administrative access to the application server must be PKI Hardware Token enabled.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35301; SV-46588

Comments:

CCI: CCI-000767The information system implements multifactor authentication for local access to privileged accounts.NIST SP 800-53 :: IA-2 (3)NIST SP 800-53A :: IA-2 (3).1NIST SP 800-53 Revision 4 :: IA-2 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must authenticate users individually prior to using a group authenticator.
STIG ID: SRG-APP-000153 **Rule ID:** SV-204748r508029_rule **Vul ID:** V-204748
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server individually authenticates users prior to authenticating via a role or group.

Review application server logs to verify user accesses requiring authentication can be traced back to an individual account.

If the application server does not authenticate users on an individual basis, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with these services to authenticate users individually prior to using a group authenticator.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure individual accountability and prevent unauthorized access, application server users (and any processes acting on behalf of application server users) must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users.

Application servers must ensure that individual users are authenticated prior to authenticating via role or group authentication. This is to ensure that there is non-repudiation for actions taken.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35302; SV-46589

Comments:

CCI: CCI-000770The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.NIST SP 800-53 :: IA-2 (5) (b)NIST SP 800-53A :: IA-2 (5).2 (ii)NIST SP 800-53 Revision 4 :: IA-2 (5)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide security extensions to extend the SOAP protocol and provide secure authentication when accessing sensitive data.
STIG ID: SRG-APP-000156 **Rule ID:** SV-204749r508029_rule **Vul ID:** V-204749
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server provides extensions to the SOAP protocol that provide secure authentication. These protocols include, but are not limited to, WS_Security suite. Review policy and data owner protection requirements in order to identify sensitive data.

If secure authentication protocols are not utilized to protect data identified by data owner as requiring protection, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch does not offer a web services capability, and it does not support SOAP/WSDL web services. Therefore, the control does not apply to Elasticsearch.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers may provide a web services capability that could be leveraged to allow remote access to sensitive application data. A web service, which is a repeatable process used to make data available to remote clients, should not be confused with a web server.

Many web services utilize SOAP, which in turn utilizes XML and HTTP as a transport. Natively, SOAP does not provide security protections. As such, the application server must provide security extensions to enhance SOAP capabilities to ensure that secure authentication mechanisms are employed to protect sensitive data. The WS_Security suite is a widely used and acceptable SOAP security extension.

Legacy Ids: V-35304; SV-46591

Comments:

CCI: CCI-001941The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.NIST SP 800-53 Revision 4 :: IA-2 (8)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must disable identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.
STIG ID: SRG-APP-000163 **Rule ID:** SV-204750r508029_rule **Vul ID:** V-204750
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to ensure the application server disables identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

If the application server is not configured to disable identifiers (individuals, groups, roles, and devices) after 35 days of inactivity, this is a finding.

Fix Text:

Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider to disable identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Inactive identifiers pose a risk to systems and applications. Attackers that are able to exploit an inactive identifier can potentially obtain and maintain undetected access to the application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Applications need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user account is the name of an information system account associated with an individual.

To avoid having to build complex user management capabilities directly into their application, wise developers leverage the underlying OS or other user account management infrastructure (AD, LDAP) that is already in place within the organization and meets organizational user

account management requirements.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35309; SV-46596

Comments:

CCI: CCI-000795The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.NIST SP 800-53 :: IA-4 eNIST SP 800-53A :: IA-4.1 (iii)NIST SP 800-53 Revision 4 :: IA-4 e

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must store only encrypted representations of passwords.
STIG ID: SRG-APP-000171 **Rule ID:** SV-204751r508029_rule **Vul ID:** V-204751
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server enforces the requirement to only store encrypted representations of passwords.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users and store only encrypted representations of passwords.

2. Additionally Password hashing settings references available for elasticsearch.yml configuration file.
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
Password hashing settings
xpack.security.authc.password_hashing.algorithm

(Static) Specifies the hashing algorithm that is used for secure user credential storage. See Table 2, “Password hashing algorithms”. Defaults to bcrypt.

3. Elasticsearch local users (native/file realm) passwords are stored salted/hashed.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html
l. Realms: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Applications must enforce password encryption when storing passwords. Passwords need to be protected at all times and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read and easily compromised.

Application servers provide either a local user store or they integrate with enterprise user stores like LDAP. When the application server is responsible for creating or storing

passwords, the application server must enforce the storage of encrypted representations of passwords.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35317; SV-46604

Comments:

CCI: CCI-000196The information system for password-based authentication stores only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must transmit only encrypted representations of passwords.
STIG ID: SRG-APP-000172 **Rule ID:** SV-204752r508029_rule **Vul ID:** V-204752
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server enforces the requirement to encrypt passwords when they are transmitted.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users. When using an IdP, Elasticsearch does not transmit user account passwords.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Encrypting communications in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
k. Encrypting communications between Elasticsearch and LDAP:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-ldap
l. Generating Node Certificates:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#node-certific
ates
m. Encrypting communications between nodes in a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-transport
n. Encrypting HTTP client communications:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-http
o. Monitoring and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-monitoring.html
p. Configuring security in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/using-kibana-with-security.html
q. Configuring security in Logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Configure Filebeat to use security features:
https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Java Client and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/java-clients.html
t. Elasticsearch for Apache Hadoop Security:
https://www.elastic.co/guide/en/elasticsearch/hadoop/8.0/security.html
u. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords during transmission. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Application servers have the capability to utilize either certificates (tokens) or user IDs and passwords in order to authenticate. When the application server transmits or receives passwords, the passwords must be encrypted.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35318; SV-46605

Comments:

CCI: CCI-000197The information system for password-based authentication transmits only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must utilize encryption when using LDAP for authentication.
STIG ID: SRG-APP-000172 **Rule ID:** SV-204753r508029_rule **Vul ID:** V-204753
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server enforces the requirement to encrypt LDAP traffic.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:

Steps/Recommendation:

When using LDAP for authentication, configure the application server to encrypt LDAP traffic.

1. Encrypt communications between Elasticsearch and LDAP. For more information, see https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html#tls-ldap

2. Configure the realm's TLS settings on each node to trust certificates signed by the CA that signed your LDAP server certificates. The following example demonstrates how to trust a CA certificate, cacert.pem, located within the Elasticsearch configuration directory (ES_PATH_CONF):

xpack:
security:
authc:
realms:
ldap:
ldap1:
order: 0
url: "ldaps://ldap.example.com:636"
ssl:
certificate_authorities: ["ES_PATH_CONF/cacert.pem"]

The CA certificate must be a PEM encoded.
You can also specify the individual server certificates rather than the CA certificate, but this is only recommended if you have a single LDAP server or the certificates are self-signed.

3. Set the url attribute in the realm configuration to specify the LDAPS protocol and the secure port number. For example, url: ldaps://ldap.example.com:636.

4. Restart Elasticsearch.

Note: By default, when you configure Elasticsearch to connect to an LDAP server using SSL/TLS, it attempts to verify the hostname or IP address specified with the url attribute in the realm configuration with the values in the certificate. If the values in the certificate and realm configuration do not match, Elasticsearch does not allow a connection to the LDAP server. This is done to protect against man-in-the-middle attacks. If necessary, you can disable this behavior by setting the ssl.verification_mode property to certificate.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Encrypting communications in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
k. Encrypting communications between Elasticsearch and LDAP:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html#tls-ldap
l. Generating Node Certificates:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#node-certificates
m. Encrypting communications between nodes in a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-transport
n. Encrypting HTTP client communications:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html#tls-http
o. Monitoring and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-monitoring.html
p. Configuring security in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/using-kibana-with-security.html
q. Configuring security in Logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Configure Filebeat to use security features:
https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Java Client and security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/java-clients.html
t. Elasticsearch for Apache Hadoop Security:
https://www.elastic.co/guide/en/elasticsearch/hadoop/8.0/security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords during transmission.

Application servers have the capability to utilize LDAP directories for authentication. If LDAP connections are not protected during transmission, sensitive authentication credentials can be stolen. When the application server utilizes LDAP, the LDAP traffic must be encrypted.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35319; SV-46606

Comments:

CCI: CCI-000197The information system for password-based authentication transmits only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must perform RFC 5280-compliant certification path validation.
STIG ID: SRG-APP-000175 **Rule ID:** SV-204754r508029_rule **Vul ID:** V-204754
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine whether the application server provides PKI functionality that validates certification paths in accordance with RFC 5280.

If PKI is not being used, this is NA.

If the application server is using PKI, but it does not perform this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. At this time, the Elastic Stack does not support RFC-5280. However, an enhancement request has been submit to add this capability to the Elastic Stack.

Reference:

a. Internal support for this is tracked in enhancement requests : https://github.com/elastic/enhancements/issues?q=is%3Aissue+is%3Aopen+CRL+

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A certificate's certification path is the path from the end entity certificate to a trusted root certification authority (CA). Certification path validation is necessary for a relying party to make an informed decision regarding acceptance of an end entity certificate. Certification path validation includes checks such as certificate issuer trust, time validity and revocation status for each certificate in the certification path. Revocation status information for CA and subject certificates in a certification path is commonly provided via certificate revocation lists (CRLs) or online certificate status protocol (OCSP) responses.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35322; SV-46609

Comments:

CCI: CCI-000185The information system for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: Only authenticated system administrators or the designated PKI Sponsor for the application server must have access to the web servers private key.
STIG ID: SRG-APP-000176 **Rule ID:** SV-204755r508029_rule **Vul ID:** V-204755
Severity: CAT II

Documentable: No

Check Content:
Review application server configuration and documentation to ensure the application server enforces authorized access to the corresponding private key.

If the application server is not configured to enforce authorized access to the corresponding private key, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.

- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and can pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys. Java-based application servers utilize the Java keystore, which provides storage for cryptographic keys and certificates. The keystore is usually maintained in a file stored on the file system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35324; SV-46611

Comments:

CCI: CCI-000186The information system for PKI-based authentication enforces authorized access to the corresponding private key.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must map the authenticated identity to the individual user or group account for PKI-based authentication.
STIG ID: SRG-APP-000177 **Rule ID:** SV-204756r508029_rule **Vul ID:** V-204756
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server provides a PKI integration capability that meets DoD PKI infrastructure requirements.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The cornerstone of PKI is the private key used to encrypt or digitally sign information. The key by itself is a cryptographic value that does not contain specific user information, but the key can be mapped to a user. Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Application servers must provide the capability to utilize and meet requirements of the DoD Enterprise PKI infrastructure for application authentication.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35325; SV-46612

Comments:

CCI: CCI-000187The information system for PKI-based authentication maps the authenticated identity to the account of the individual or group.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
STIG ID: SRG-APP-000178 **Rule ID:** SV-204757r508029_rule **Vul ID:** V-204757
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if any interfaces which are provided for authentication purposes display the user's password when it is typed

into the data entry field.

If authentication information is not obfuscated when entered, this is a finding.

Fix Text:
Steps/Recommendation:

1. Kibana can be used as the front end, to prohibit the display of passwords in clear text on the command line.

2. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI). The recommendation is to integrate Elasticsearch with these services to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

References:

a. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. Rest APIs: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/rest-apis.html
c. Kibana Guide: https://www.elastic.co/guide/en/kibana/8.0/index.html
d. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To prevent the compromise of authentication information during the

authentication process, the application server authentication screens must obfuscate input so an unauthorized user cannot view a password, PIN, or any other authenticator value as it is being typed.

This can occur when a user is authenticating to the application server through the web management interface or command line interface. The application server must obfuscate all passwords, PINs, or other authenticator information when typed. User ID is not required to be obfuscated.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-35328; SV-46615

Comments:

CCI: CCI-000206The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.NIST SP 800-53 :: IA-6NIST SP 800-53A :: IA-6.1NIST SP 800-53 Revision 4 :: IA-6

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must utilize FIPS 140-2 approved encryption modules when authenticating users and processes.
STIG ID: SRG-APP-000179 **Rule ID:** SV-204758r508029_rule **Vul ID:** V-204758
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine which version of TLS is being used.

If the application server is not using TLS when authenticating users or non-FIPS-approved SSL versions are enabled, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security

(TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html

i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Encryption is only as good as the encryption modules utilized. Unapproved cryptographic module algorithms cannot be verified and cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised due to weak algorithms. The use of TLS provides confidentiality of data in transit between the application server and client.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-35329; SV-46616

Comments:

CCI: CCI-000803The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.NIST SP 800-53 :: IA-7NIST SP 800-53A :: IA-7.1NIST SP 800-53 Revision 4 :: IA-7

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful logon attempts occur.
STIG ID: SRG-APP-000503 **Rule ID:** SV-204826r508029_rule **Vul ID:** V-204826
Severity: CAT II

Documentable: No

Check Content:
Review product documentation and the system configuration to determine if the application server generates log records on successful and unsuccessful logon attempts by users.

If logon attempts do not generate log records, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Logging the access to the application server allows the system administrators to monitor user accounts. By logging successful/unsuccessful logons, the system administrator can determine if an account is compromised (e.g., frequent logons) or is in the process of being compromised (e.g., frequent failed logons) and can take actions to thwart the attack.

Logging successful logons can also be used to determine accounts that are no longer in use.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57443; SV-71715

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide a log reduction capability that supports on-demand reporting requirements.
STIG ID: SRG-APP-000181 **Rule ID:** SV-204759r508029_rule **Vul ID:** V-204759
Severity: CAT II

Documentable: No

Check Content:
Review application server product documentation and server configuration to determine if the application server is configured to provide log reduction with on-demand reporting.

If the application server is not configured to provide log reduction with on-demand reporting, or is not configured to send its logs to a centralized log system, this is a finding.

Fix Text:
Steps/Recommendation:

1. You can use the Elasticsearch APIs to perform on-demand reporting.
curl -X GET "localhost:9200/my-index-000001/_search?pretty"

2. Recommend usage of Kibana UI and Beats dashboards for a more robust user experience.

References:

a. Search: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
b. Mapping -> Mapping Parameters -> fielddata:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fielddata.html
c. Index and Search Analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html
d. Kibana Query: https://www.elastic.co/guide/en/kibana/8.0/kuery-query.html
e. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
f. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: The ability to generate on-demand reports, including after the log data has been subjected to log reduction, greatly facilitates the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Log reduction is a process that manipulates collected log information and organizes such information in a summary format that is more meaningful to analysts. The report generation capability provided by the application must support on-demand (i.e., customizable, ad-hoc, and as needed) reports.

Instead of the application server providing the log reduction function; it is also accepted practice to configure the application server to send its logs to a centralized log system that can be used to provide the log reduction with reporting capability. Security Incident Event Management (SIEM) systems are an example of such a solution.

To fully understand and investigate an incident within the components of the application server, the application server, must be configured to provide log reduction and on-demand reporting or be configured to send its logs to a centralized log system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57527; SV-71803

Comments:

CCI: CCI-001876The information system provides an audit reduction capability that supports on-demand reporting requirements.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records for privileged activities.
STIG ID: SRG-APP-000504 **Rule ID:** SV-204827r508029_rule **Vul ID:** V-204827
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records for privileged activities.

If log records are not generated for privileged activities, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Privileged activities would occur through the management interface. This interface can be web-based or can be command line utilities. Whichever method is utilized by the application server, these activities must be logged.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57445; SV-71717

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must identify prohibited mobile code.
STIG ID: SRG-APP-000206 **Rule ID:** SV-204760r508029_rule **Vul ID:** V-204760
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server is configured to identify prohibited mobile code.

If the application server is not configured to identify prohibited mobile code, this is a finding.

Fix Text:

Step/Recommendation:

1. For the Elastic-hosted Elasticsearch Service, per 800-53 (SC-18 Mobile Code), Elasticsearch service currently does not make use of mobile code and has set no usage restrictions of mobile code (e.g., JavaScript, VBScript, ActiveX, etc.) within the Elastic Cloud application, although protections are configured to identify anomalous activity. An end user's workstation should have endpoint protection and browser controls implemented to prevent the execution of unauthorized mobile code.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Mobile code is defined as software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

Mobile code technologies include: Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

Application servers must meet policy requirements regarding the deployment and/or use of mobile code. This includes digitally signing applets in order to provide a means for the client to establish application authenticity and prohibit unauthorized code from being used.

Legacy Ids: V-57547; SV-71823

Comments:

CCI: CCI-001166The information system identifies organization-defined unacceptable mobile code.NIST SP 800-53 :: SC-18 (1)NIST SP 800-53A :: SC-18 (1).1 (i)NIST SP 800-53 Revision 4 :: SC-18 (1)

Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application must generate log records showing starting and ending times for user access to the application server management interface.
STIG ID: SRG-APP-000505 **Rule ID:** SV-204828r508029_rule **Vul ID:** V-204828
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records showing starting and ending times for user access to the management interface.

If log records are not generated showing starting and ending times of user access to the management interface, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Determining when a user has accessed the management interface is important to determine the timeline of events when a security incident occurs. Generating these events, especially if the management interface is accessed via a stateless protocol like HTTP, the log events will be generated when the user performs a logon (start) and when the user performs a logoff (end). Without these events, the user and later investigators cannot determine the sequence of events and therefore cannot determine what may have happened and by whom it may have been done.

The generation of start and end times within log events allow the user to perform their due diligence in the event of a security breach.

Legacy Ids: V-57481; SV-71757

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must separate hosted application functionality from application server management functionality.

STIG ID: SRG-APP-000211 **Rule ID:** SV-204761r508029_rule **Vul ID:** V-204761
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to verify that the application server separates admin functionality from hosted application functionality.

If the application server does not separate application server admin functionality from hosted application functionality, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch natively does not provide a GUI interface. Recommended to use the Kibana UI for managing the Elastic Stack.

Access to individual features is governed by Elasticsearch and Kibana privileges.

2. The separation of user functionality from application server management can be accomplished by moving management functions to a separate IP address or port—a separate Kibana space for administrative functions and another separate space for end user-related functionality.

Each Elasticsearch node has two different network interfaces. Clients send requests to Elasticsearch's REST APIs using its HTTP interface, but nodes communicate with other nodes using the transport interface. The transport interface is also used for communication with remote clusters.

Transport settings
The following settings can be configured for the internal transport that communicates over TCP. Some of the available settings are presented below for brevity.

transport.port
(Static) The port to bind for communication between nodes. Accepts a single value or a range. If a range is specified, the node will bind to the first available port in the range. Set this setting to a single port, not a range, on every master-eligible node.
Defaults to 9300-9400.

transport.publish_port
(Static) The port of the transport publish address. Set this parameter only if you need the publish port to be different from transport.port. Defaults to the port assigned via transport.port.

transport.bind_host
(Static) The network address(es) to which the node should bind in order to listen for incoming transport connections. Accepts a list of IP addresses, hostnames, and special values. Defaults to the address given by transport.host or network.bind_host. Use this setting only if you require to bind to multiple addresses or to use different addresses for publishing and binding, and you also require different binding configurations for the transport and HTTP interfaces.

transport.publish_host
(Static) The network address at which the node can be contacted by other nodes. Accepts an IP address, a hostname, or a special value. Defaults to the address given by transport.host or network.publish_host. Use this setting only if you require to bind to multiple addresses or to use different addresses for publishing and binding, and you also require different binding configurations for the transport and HTTP interfaces.

transport.host
(Static) Sets the address of this node for transport traffic. The node will bind to this address and will also use it as its transport publish address. Accepts an IP address, a hostname, or a special value. Use this setting only if you require different configurations for the transport and HTTP interfaces.

Defaults to the address given by network.host.

3. The separation of user functionality from application server management can be accomplished by creating separate Kibana spaces for administrative functions and another separate space for end user-related functionality.

Spaces can be managed via the Kibana interface through the main menu, Stack Management > Spaces. This view provides actions to create, edit, and delete spaces.

References:

a. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html
b. Networking:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-network.html
c. Kibana spaces: https://www.elastic.co/guide/en/kibana/master/xpack-spaces.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server consists of the management interface and hosted applications. By separating the management interface from hosted applications, the user must

authenticate as a privileged user to the management interface before being presented with management functionality. This prevents non-privileged users from having visibility to functions not available to the user. By limiting visibility, a compromised non-privileged account does not offer information to the attacker to functionality and information needed to further the attack on the application server.

Application server management functionality includes functions necessary to administer the application server and requires privileged access via one of the accounts assigned to a management role. The hosted application and hosted application functionality consists of the assets needed for the application to function, such as the business logic, databases, user authentication, etc.

The separation of application server administration functionality from hosted application functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, network addresses, network ports, or combinations of these methods, as appropriate.

Legacy Ids: V-35376; SV-46663

Comments:

CCI: CCI-001082The information system separates user functionality (including user interface services) from information system management functionality.NIST SP 800-53 :: SC-2NIST SP 800-53A :: SC-2.1NIST SP 800-53 Revision 4 :: SC-2

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when concurrent logons from different workstations occur to the application server management interface.
STIG ID: SRG-APP-000506 **Rule ID:** SV-204829r508029_rule **Vul ID:** V-204829
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records showing concurrent logons from different workstations to the management interface.

If concurrent logons from different workstations are not logged, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: Being able to work on a system through multiple views into the application allows a user to work more efficiently and more accurately. Before environments with windowing capabilities or multiple desktops, a user would log onto the application from different workstations or terminals. With today's workstations, this is no longer necessary and may signal a compromised session or user account.

When concurrent logons are made from different workstations to the management interface, a log record needs to be generated. This allows the system administrator to investigate the incident and to be aware of the incident.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57483; SV-71759

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured to mutually authenticate connecting proxies, application servers or gateways.
STIG ID: SRG-APP-000219 **Rule ID:** SV-204762r508029_rule **Vul ID:** V-204762
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation, system security plan and application data protection requirements.

If the connected web proxy is exposed to an untrusted network or if data protection requirements specified in the system security plan mandate the need to establish the identity of the connecting application server, proxy or application gateway and the application server is not configured to mutually authenticate the application server, proxy server or gateway, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports mutual TLS for the HTTP layer. A proxy should be placed in front of the cluster to satisfy this control, which can be configured for mTLS with Elasticsearch.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application architecture may sometimes require a configuration where an application server is placed behind a web proxy, an application gateway or communicates directly with another application server. In those instances, the application server hosting the service/application is considered the server. The application server, proxy or application gateway consuming the hosted service is considered a client. Authentication is accomplished via the use of certificates and protocols such as TLS mutual authentication. Authentication must be performed when the proxy is exposed to an untrusted network or when data protection requirements specified in the system security plan mandate the need to establish the identity of the connecting application server, proxy or application gateway.

Connect clients to Elasticsearch:
When you start Elasticsearch for the first time, TLS is configured automatically for the HTTP layer. A CA certificate is generated and stored on disk at $ES_HOME/config/certs/http_ca.crt. The hex-encoded SHA-256 fingerprint of this certificate is also output to the terminal. Any clients that connect to Elasticsearch, such as the Elasticsearch Clients, Beats, standalone Elastic Agents, and Logstash must validate that they trust the certificate that Elasticsearch uses for HTTPS. Fleet Server and Fleet-managed Elastic Agents are automatically configured to trust the CA certificate. Other clients can establish trust by using either the fingerprint of the CA certificate or the CA certificate itself.

Start the Elastic Stack with security:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Legacy Ids: V-35381; SV-46668

Comments:

CCI: CCI-001184The information system protects the authenticity of communications sessions.NIST SP 800-53 :: SC-23NIST SP 800-53A :: SC-23.1NIST SP 800-53 Revision 4 :: SC-23

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records for all account creations, modifications, disabling, and termination events.
STIG ID: SRG-APP-000509 **Rule ID:** SV-204830r508029_rule **Vul ID:** V-204830
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when accounts are created, modified, disabled, or terminated.

If the application server does not generate log records for account creation, modification, disabling, and termination, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The maintenance of user accounts is a key activity within the system to determine access and privileges. Through changes to accounts, an attacker can create an account for persistent access, modify an account to elevate privileges or terminate/disable an account(s) to cause a DoS for user(s). To be able to track and investigate these actions, log records must be generated for any account modification functions.

Application servers either provide a local user store, or they can integrate with enterprise user stores like LDAP. As such, the application server must be able to generate log records on account creation, modification, disabling, and termination.

Legacy Ids: V-57485; SV-71761

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must invalidate session identifiers upon user logout or other session termination.
STIG ID: SRG-APP-000220 **Rule ID:** SV-204763r508029_rule **Vul ID:** V-204763
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and organizational policy to determine if the system is configured to terminate administrator sessions upon administrator logout or any other organization- or policy-defined session termination events, such as idle time limit exceeded.

If the configuration is not set to terminate administrator sessions per defined events, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to invalidate session identifiers upon user logout or other session termination or any other organization- or policy-defined session termination events.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html

d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If communications sessions remain open for extended periods of time even when unused, there is the potential for an adversary to hijack the session and use it to gain access to the device or networks to which it is attached. Terminating sessions after a logout event or after a certain period of inactivity is a method for mitigating the risk of this vulnerability. When a user management session becomes idle, or when a user logs out of the management interface, the application server must terminate the session.

Legacy Ids: V-35415; SV-46702

Comments:

CCI: CCI-001185The information system invalidates session identifiers upon user logout or other session termination.NIST SP 800-53 :: SC-23 (1)NIST SP 800-53A :: SC-23 (1).1NIST SP 800-53 Revision 4 :: SC-23 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: Application servers must use NIST-approved or NSA-approved key management technology and processes.
STIG ID: SRG-APP-000514 **Rule ID:** SV-204831r508029_rule **Vul ID:** V-204831
Severity: CAT II

Documentable: No

Check Content:
Review application server configuration and the NIST FIPS certificate to validate the application server uses NIST-approved or NSA-approved key management technology and processes when producing, controlling or distributing symmetric and asymmetric keys.

If the application server does not use this NIST-approved or NSA-approved key management technology and processes, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the

Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: An asymmetric encryption key must be protected during transmission. The public portion of an asymmetric key pair can be freely distributed without fear of compromise, and the private portion of the key must be protected. The application server will provide software libraries that applications can programmatically utilize to encrypt and decrypt information. These application server libraries must use NIST-approved or NSA-approved key management technology and processes when producing, controlling, or distributing symmetric and asymmetric keys.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57543; SV-71819

Comments:

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations and standards.NIST SP 800-53 Revision 4 :: SC-13

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate a unique session identifier for each session.
STIG ID: SRG-APP-000223 **Rule ID:** SV-204764r508029_rule **Vul ID:** V-204764
Severity: CAT II

Documentable: No

Check Content:
Review the application server session management configuration settings in either the application server management console, application server initialization or application server configuration files to determine if the application server is configured to generate a unique session identifier for each session.

If the application server is not configured to generate a unique session identifier for each session, this is a finding.

Fix Text:

Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to generate a unique session identifier for each session.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Unique session IDs are the opposite of sequentially generated session IDs, which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of session identifiers. Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have

more difficulty in hijacking the session or otherwise manipulating valid sessions.

Application servers must generate a unique session identifier for each application session so as to prevent session hijacking.

Legacy Ids: V-57549; SV-71825

Comments:

CCI: CCI-001664The information system recognizes only session identifiers that are system-generated.NIST SP 800-53 :: SC-23 (3)NIST SP 800-53A :: SC-23 (3).1 (ii)NIST SP 800-53 Revision 4 :: SC-23 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must recognize only system-generated session identifiers.
STIG ID: SRG-APP-000223 **Rule ID:** SV-204765r508029_rule **Vul ID:** V-204765
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server recognizes only system-generated session identifiers.

If the application server does not recognize only system-generated session identifiers, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to recognize only system-generated session identifiers.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This requirement focuses on communications protection at the application session, versus network packet level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted.

Unique session IDs are the opposite of sequentially generated session IDs which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of said identifiers.

Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

Legacy Ids: V-35421; SV-46708

Comments:

CCI: CCI-001664The information system recognizes only session identifiers that are system-generated.NIST SP 800-53 :: SC-23 (3)NIST SP 800-53A :: SC-23 (3).1 (ii)NIST SP

800-53 Revision 4 :: SC-23 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use DoD- or CNSS-approved PKI Class 3 or Class 4 certificates.
STIG ID: SRG-APP-000514 **Rule ID:** SV-204832r508029_rule **Vul ID:** V-204832
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server utilizes approved PKI Class 3 or Class 4 certificates.

If the application server is not configured to use approved DoD or CNS certificates, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Use a DoD PKI Class 3 or Class 4 certificate in both Elasticsearch and Kibana.

3. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

4. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

5. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

6. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:

- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac

r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Class 3 PKI certificates are used for servers and software signing rather than for identifying individuals. Class 4 certificates are used for business-to-business transactions. Utilizing unapproved certificates not issued or approved by DoD or CNS creates an integrity risk. The application server must utilize approved DoD or CNS Class 3 or Class 4 certificates for software signing and business-to-business transactions.

Legacy Ids: V-57545; SV-71821

Comments:

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.NIST SP 800-53 Revision 4 :: SC-13

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate a unique session identifier using a FIPS 140-2 approved random number generator.
STIG ID: SRG-APP-000224 **Rule ID:** SV-204766r508029_rule **Vul ID:** V-204766
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and documentation to determine if the application server uses a FIPS 140-2 approved random number generator to create unique session identifiers.

Have a user log onto the application server to determine if the session IDs generated are random and unique.

If the application server does not generate unique session identifiers and does not use a FIPS 140-2 random number generator to create the randomness of the session ID, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to generate a unique session identifier using a FIPS 140-2 approved random number generator.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server will use session IDs to communicate between modules or applications within the application server and between the application server and users. The session ID allows the application to track the communications along with credentials that may have been used to authenticate users or modules.

Unique session IDs are the opposite of sequentially generated session IDs which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of said identifiers.

Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

Legacy Ids: V-35422; SV-46709

Comments:

CCI: CCI-001188The information system generates unique session identifiers for each session with organization-defined randomness requirements.NIST SP 800-53 :: SC-23 (4)NIST SP 800-53A :: SC-23 (4).1 (ii)NIST SP 800-53 Revision 4 :: SC-23 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must, at a minimum, transfer the logs of interconnected systems in real time, and transfer the logs of standalone systems weekly.
STIG ID: SRG-APP-000515 **Rule ID:** SV-204833r508029_rule **Vul ID:** V-204833
Severity: CAT II

Documentable: No

Check Content:
Verify the log records are being off-loaded, at a minimum of real time for interconnected systems and weekly for standalone systems.

If the application server is not meeting these requirements, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch can be configured to provide redundancy by storing the Elasticsearch data on different media to support off-load interconnected systems in real time and off-load

standalone systems weekly, at a minimum. Verify that standalone system logs are received when those systems are re-connected and automatically resumed when connectivity is restored after a loss in connectivity.

Reference:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/current/resiliency.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration. Protecting log data is important during a forensic investigation to ensure investigators can track and understand what may have occurred. Off-loading should be set up as a scheduled task but can be configured to be run manually, if other processes during the off-loading are manual.

Off-loading is a common process in information systems with limited log storage capacity.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57425; SV-71697

Comments:

CCI: CCI-001851The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.NIST SP 800-53 Revision 4 :: AU-4 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured to perform complete application deployments.
STIG ID: SRG-APP-000225 **Rule ID:** SV-204767r508029_rule **Vul ID:** V-204767
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and documentation to ensure the system is configured to perform complete application deployments.

If the application server is not configured to ensure complete application deployments or provides no rollback functionality, this is a finding.

Fix Text:
Steps/Recommendation:

1. As part of the hosted Elasticsearch Service offering, customers may configure how they wish to run backups to enable rollback or restore of their configurations. Elastic is responsible for SaaS and system wide capabilities for snapshot and restore operations at the SaaS layer level. Use of ECE, ECK, or Elastic Cloud is recommended; rollback or prevention of deployment if errors are encountered is not supported by Elastic for "self-managed" implementations.

ECE supports rolling upgrades on an Elasticsearch cluster to be upgraded one node at a time so upgrading does not interrupt service.

Note: When upgrading to Elasticsearch 8.0 and later, you must first upgrade to 7.17 whether you opt to perform a rolling upgrade (upgrade one node at a time) or a full-cluster restart upgrade.

Before you start to upgrade your cluster you should do the following.
- Check the deprecation log to see if you are using any deprecated features and update your code accordingly.
- Review the breaking changes and make any necessary changes to your code and configuration for version.
- If you use any plugins, make sure there is a version of each plugin that is compatible with Elasticsearch version.
- Test the upgrade in an isolated environment before upgrading your production cluster.
- Back up your data by taking a snapshot!

2. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to enable rollback or restore to the last known good configuration in the event of errors that occur during application deployment and to prevent deployment if errors are encountered.

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

b. Rolling upgrades:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/rolling-upgrades.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system.

When an application is deployed to the application server, if the deployment process does not complete properly and without errors, there is the potential that some application files may not be deployed or may be corrupted and an application error may occur during runtime.

The application server must be able to perform complete application deployments. A partial deployment can leave the server in an inconsistent state. Application servers may provide a transaction rollback function to address this issue.

Legacy Ids: V-35423; SV-46710

Comments:

CCI: CCI-001190The information system fails to an organization-defined known-state for organization-defined types of failures.NIST SP 800-53 :: SC-24NIST SP 800-53A :: SC-24.1 (iv)NIST SP 800-53 Revision 4 :: SC-24

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.
STIG ID: SRG-APP-000516 **Rule ID:** SV-204834r508029_rule **Vul ID:** V-204834
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application

server is configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.

If the application server is not configured in accordance with security configuration settings, this is a finding.

Fix Text:
Step/Recommendation:

1. It is up to the organization to ensure the application server is configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including Security Technical Implementation (STIGs), NSA configuration guides, CYBERCOM Task Order (CTOs), and Directive-Type Memorandum (DTM).

References:

a. STIGs: https://cyber.mil/stigs/
b. NSA Configuration Guides:
https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/
c. CTOs: https://www.cybercom.mil/
d. DTMs: https://www.esd.whs.mil/DD/DoD-Issuances/DTM/

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Configuring the application to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the application, including the parameters required to satisfy other security control requirements.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57499; SV-71775

Comments:

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide a clustering capability.
STIG ID: SRG-APP-000225 **Rule ID:** SV-204768r508029_rule **Vul ID:** V-204768
Severity: CAT II

Documentable: No

Check Content:
This requirement is dependent upon system MAC and confidentiality.

If the system MAC and confidentiality levels do not specify redundancy requirements, this requirement is NA.

Review the application server configuration and documentation to ensure the application server is configured to provide clustering functionality.

If the application server is not configured to provide clustering or some form of failover functionality, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch provides a clustering capability by design.
A single instance of Elasticsearch is a node. A collection of connected nodes is called a cluster.

Nodes are added to a cluster to increase its capacity and reliability. By default, a node is both a data node and eligible to be elected as the master node that controls the cluster. A node can be configured for a specific purpose, such as handling ingest requests.

By default, a node is all of the following types: master-eligible, data, ingest, and (if available) machine learning. All data nodes are also transform nodes.

As the cluster grows and in particular if you have large machine learning jobs or continuous transforms, consider separating dedicated master-eligible nodes from dedicated data nodes,

machine learning nodes, and transform nodes.

Node roles can be defined by setting node.roles. If this is not set, then the node has the following roles by default:

master
data
data_content
data_hot
data_warm
data_cold
data_frozen
ingest
ml
remote_cluster_client
transform

References:

a. Add and remove nodes in your cluster: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This requirement is dependent upon system MAC and confidentiality. If the system MAC and confidentiality levels do not specify redundancy requirements, this requirement is NA.

Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. When application failure is encountered, preserving application state facilitates application restart and return to the operational mode of the organization with less disruption of mission/business processes.

Clustering of multiple application servers is a common approach to providing fail-safe application availability when system MAC and confidentiality levels require redundancy.

Legacy Ids: V-35424; SV-46711

Comments:

CCI: CCI-001190The information system fails to an organization-defined known-state for organization-defined types of failures.NIST SP 800-53 :: SC-24NIST SP 800-53A :: SC-24.1 (iv)NIST SP 800-53 Revision 4 :: SC-24

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
STIG ID: SRG-APP-000416 **Rule ID:** SV-220326r508029_rule **Vul ID:** V-220326
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to verify that the application server is using NSA-approved cryptography to protect classified data and applications resident on the device.

If the application server is not using NSA-approved cryptography for classified data and applications, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Cryptography is only as strong as the encryption modules/algorithms employed to encrypt the data. Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data.

NSA has developed Type 1 algorithms for protecting classified information. The Committee on National Security Systems (CNSS) National Information Assurance Glossary (CNSS Instruction No. 4009) defines Type 1 products as:

"Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA-approved algorithms
are used to protect systems requiring the most stringent protection mechanisms."

NSA-approved cryptography is required to be used for classified information system processing.

The application server must utilize NSA-approved encryption modules when protecting classified data. This means using AES and other approved encryption modules.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57541; SV-71817

Comments:

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.NIST SP 800-53 Revision 4 :: SC-13

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.
STIG ID: SRG-APP-000225 **Rule ID:** SV-204769r508029_rule **Vul ID:** V-204769
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server fails to a secure state if system initialization fails, shutdown fails, or aborts fail.

If the application server cannot be configured to fail securely, this is a finding.

Fix Text:
Steps/Recommendation:

Elasticsearch does not currently offer to fail to a secure state if system initialization fails, shutdown fails, or aborts fail; in that the way to shut down a node is to terminate the process.

Recommend configuring Elasticsearch for high availability. The system will fail over to the backup capability as part of the customer contingency plan, in which case, the system doesn't "fail" and the customer can investigate the primary component's status without interruption of service.

1. Elasticsearch provides a clustering capability by design and can be configured in a high-availability (HA) cluster. Elasticsearch offers a number of features to achieve HA despite failures.

- With proper planning, a cluster can be designed for resilience to many of the things that commonly go wrong, from the loss of a single node or network connection right up to a zone-wide outage such as power loss.
- Use cross-cluster replication to replicate data to a remote follower cluster which may be in a different data centre or even on a different continent from the leader cluster. The follower cluster acts as a hot standby, ready fail over in the event of a disaster so severe that the leader cluster fails. The follower cluster can also act as a geo-replica to serve searches from nearby

clients.
- The last line of defense against data loss is to take regular snapshots of the cluster so that it can be restored elsewhere if needed.

Designing for resilience
A resilient cluster requires redundancy for every required cluster component. This means a resilient cluster must have:
- At least three master-eligible nodes
- At least two nodes of each role
- At least two copies of each shard (one primary and one or more replicas)

Back up a cluster
To have a complete backup for a cluster:
- Back up the data
- Back up the cluster configuration
- Back up the security configuration

2. If using Elasticsearch as a SaaS product (Elastic-hosted), recommend a minimum of three availability zones to enable Elastic Cloud Enterprise to create clusters with a tiebreaker.

High availability
- Fault tolerance for Elastic Cloud Enterprise is based around the concept of availability zones.
- An availability zone contains resources available to an Elastic Cloud Enterprise installation that are isolated from other availability zones to safeguard against potential failure.
- If there are only two availability zones in total in an installation, no tiebreaker is created.

3. Refer to the cloud provider options of Regions and Availability Zones for high-availability (HA) cluster for hosting the Elastic cluster.

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html
c. Set up a cluster for high availability:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability.html
d. Designing for resilience:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability-cluster-design.html
e. Cross-cluster replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html
f. Create a snapshot:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/snapshots-take-snapshot.html
g. High availability: https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-ha.html
h. Bootstrap Checks:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/bootstrap-checks.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Fail-secure is a condition achieved by the application server in order to ensure that in the event of an operational failure, the system does not enter into an unsecure state where intended security properties no longer hold. Preserving information system state information also facilitates system restart and return to the operational mode of the organization with less disruption of mission-essential processes.

Legacy Ids: V-57553; SV-71829

Comments:

CCI: CCI-001190The information system fails to an organization-defined known-state for organization-defined types of failures.NIST SP 800-53 :: SC-24NIST SP 800-53A :: SC-24.1 (iv)NIST SP 800-53 Revision 4 :: SC-24

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect the confidentiality and integrity of all information at rest.
STIG ID: SRG-APP-000231 **Rule ID:** SV-204770r508029_rule **Vul ID:** V-204770
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to ensure the application server is protecting the confidentiality and integrity of all information at rest.

If the confidentiality and integrity of all information at rest is not protected, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch

Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When data is written to digital media such as hard drives, mobile computers, external/removable hard drives, personal digital assistants, flash/thumb drives, etc., there is risk of data loss and data compromise.

Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed the physical access controls where the media resides provide adequate protection.

As part of a defense-in-depth strategy, data owners and DoD consider routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information.

The strength of mechanisms is commensurate with the classification and sensitivity of the information.

The application server must directly provide, or provide access to, cryptographic libraries and functionality that allow applications to encrypt data when it is stored.

Legacy Ids: V-57555; SV-71831

Comments:

CCI: CCI-001199The information system protects the confidentiality and/or integrity of organization-defined information at rest.NIST SP 800-53 :: SC-28NIST SP 800-53A :: SC-28.1NIST SP 800-53 Revision 4 :: SC-28

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must employ cryptographic mechanisms to ensure confidentiality and integrity of all information at rest when stored off-line.
STIG ID: SRG-APP-000231 **Rule ID:** SV-204771r508029_rule **Vul ID:** V-204771
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to ensure the system is protecting the confidentiality and integrity of all application server data at rest when stored off-line.

If the application server is not configured to protect all application server data at rest when stored off-line, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html

d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.

Application servers generate information throughout the course of their use, most notably, log data. If the data is not encrypted while at rest, the data used later for forensic investigation cannot be guaranteed to be unchanged and cannot be used for prosecution of an attacker. To accomplish a credible investigation and prosecution, the data integrity and information confidentiality must be guaranteed.

Application servers must provide the capability to protect all data, especially log data, so as to ensure confidentiality and integrity.

Legacy Ids: V-35426; SV-46713

Comments:

CCI: CCI-001199The information system protects the confidentiality and/or integrity of organization-defined information at rest.NIST SP 800-53 :: SC-28NIST SP 800-53A :: SC-28.1NIST SP 800-53 Revision 4 :: SC-28

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must check the validity of all data inputs to the management interface, except those specifically identified by the organization.
STIG ID: SRG-APP-000251 **Rule ID:** SV-204772r508029_rule **Vul ID:** V-204772
Severity: CAT II

Documentable: No

Check Content:

Review the application server configuration to determine if the system checks the validity of information inputs to the management interface, except those specifically identified by the organization.

If the management interface data inputs are not validated, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommended using the Kibana UI to manage the Elastic Stack and that Kibana performs input validation checks. Access to individual features is governed by Elasticsearch and Kibana privileges.

References:

a. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html
b. Security best practices:
https://www.elastic.co/guide/en/kibana/8.0/security-best-practices.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Invalid user input occurs when a user inserts data or characters into an applications data entry field and the application is unprepared to process that data. This results in unanticipated application behavior potentially leading to an application or information system compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

Application servers must ensure their management interfaces perform data input validation checks. Input validation consists of evaluating user input and ensuring that only allowed characters are utilized. An example is ensuring that the interfaces are not susceptible to SQL injection attacks.

Legacy Ids: V-35436; SV-46723

Comments:

CCI: CCI-001310The information system checks the validity of organization-defined inputs.NIST SP 800-53 :: SI-10NIST SP 800-53A :: SI-10.1NIST SP 800-53 Revision 4 :: SI-10

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must identify potentially security-relevant error conditions.
STIG ID: SRG-APP-000266 **Rule ID:** SV-204773r508029_rule **Vul ID:** V-204773
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the system identifies potentially security-relevant error conditions on the server.

If this function is not performed, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the application server to generate log records for potentially security-relevant error conditions like when successful/unsuccessful attempts to modify privileges occur.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to generate

log records for potentially security-relevant error conditions like when successful/unsuccessful attempts to modify privileges occur.

4. Recommend establishing an alert to appropriate personnel for potentially security-relevant error conditions.

The Elastic Stack API can be used to setup alerts. However, it is recommended to use the Kibana UI for a better user experience.

5. Watcher
The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. They can be tailor to meet specific needs.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
e. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/how-monitoring-works.html
f. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
g. Kibana Alerts: https://www.elastic.co/guide/en/kibana/8.0/kibana-alerts.html
h. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
i. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
j. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
k. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
l. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
m. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
n. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
o. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
p. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html

q. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
r. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
s. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
t. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The structure and content of error messages need to be carefully considered by the organization and development team. Any application providing too much information in error logs and in administrative messages to the screen risks compromising the data and security of the application and system. The extent to which the application server is able to identify and handle error conditions is guided by organizational policy and operational requirements. Adequate logging levels and system performance capabilities need to be balanced with data protection requirements.

The structure and content of error messages needs to be carefully considered by the organization and development team.

Application servers must have the capability to log at various levels which can provide log entries for potential security-related error events.

An example is the capability for the application server to assign a criticality level to a failed logon attempt error message, a security-related error message being of a higher criticality.

Legacy Ids: V-57567; SV-71843

Comments:

CCI: CCI-001312The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.NIST SP 800-53 :: SI-11 bNIST SP 800-53A :: SI-11.1 (iii)NIST SP 800-53 Revision 4 :: SI-11 a

Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must only generate error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages.
STIG ID: SRG-APP-000266 **Rule ID:** SV-204774r508029_rule **Vul ID:** V-204774
Severity: CAT II

Documentable: No

Check Content:
Review system documentation and logs to determine if the application server writes sensitive information such as passwords or private keys into the logs and administrative messages.

If the application server writes sensitive or potentially harmful information into the logs and administrative messages, this is a finding.

Fix Text:
Steps/Recommendation:

1. End users will typically see very generic error messages designed to be brief and high level. The default logging level of Elasticsearch and Kibana adheres to the control.

2. Configure any custom application code not to divulge sensitive information or information useful for system identification in the error information.

References:

a. Logging: https://www.elastic.co/guide/en/elasticsearch/reference/current/logging.html
b. Kibana reporting troubleshooting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-troubleshooting.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Any application providing too much information in error logs and in administrative messages to the screen risks compromising the data and security of the application and system. The structure and content of error messages needs to be carefully considered by the organization and development team.

The application server must not log sensitive information such as passwords, private keys, or

other sensitive data. This requirement pertains to logs that are generated by the application server and application server processes, not the applications that may reside on the application server. Those errors are out of the scope of these requirements.

Legacy Ids: V-35440; SV-46727

Comments:

CCI: CCI-001312The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.NIST SP 800-53 :: SI-11 bNIST SP 800-53A :: SI-11.1 (iii)NIST SP 800-53 Revision 4 :: SI-11 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must restrict error messages only to authorized users.
STIG ID: SRG-APP-000267 **Rule ID:** SV-204775r508029_rule **Vul ID:** V-204775
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration and documentation to determine if the application server will restrict access to error messages so only authorized users may view or otherwise access them.

If the application server cannot be configured to restrict access to error messages to only authorized users, this is a finding.

Fix Text:
Steps/Recommendation:

1. End users will typically see very generic error messages designed to be brief and high level. The default logging level of Elasticsearch and Kibana adheres to the control.

Configure any custom application code not to divulge sensitive information or information useful for system identification in the error information.

2. Enabling security protects Elasticsearch clusters by preventing unauthorized access with password protection, role-based access control, and IP filtering. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

References:

a. Logging: https://www.elastic.co/guide/en/elasticsearch/reference/current/logging.html
b. Kibana reporting troubleshooting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-troubleshooting.html
c. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html
d. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the application provides too much information in error logs and administrative messages to the screen, this could lead to compromise. The structure and content of error messages need to be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Application servers must protect the error messages that are created by the application server. All application server users' accounts are used for the management of the server and the applications residing on the application server. All accounts are assigned to a certain role with corresponding access rights. The application server must restrict access to error messages so only authorized users may view them. Error messages are usually written to logs contained on the file system. The application server will usually create new log files as needed and must take steps to ensure that the proper file permissions are utilized when the log files are created.

Legacy Ids: V-35441; SV-46728

Comments:

CCI: CCI-001314The information system reveals error messages only to organization-defined personnel or roles.NIST SP 800-53 :: SI-11 cNIST SP 800-53A :: SI-11.1 (iv)NIST SP 800-53 Revision 4 :: SI-11 b

Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must use cryptographic mechanisms to protect the integrity of log tools.
STIG ID: SRG-APP-000290 **Rule ID:** SV-204776r508029_rule **Vul ID:** V-204776
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server log tools have been cryptographically signed to protect the integrity of the tools.

If the application server log tools have not been cryptographically signed, this is a finding.

Fix Text:
Steps/Recommendation:

Currently, Elastic does not sign any of the jars/code in Elasticsearch.

1. For the Elastic cloud hosted service offerings, Elastic uses Auditbeat and Elastic Endpoint Security as host-based intrusion detection system and File Integrity Management (HIDS)/(FIM) on all hosts, specifying files and directories to be monitored for changes. File changes are detected in near real time and sent to Elasticsearch clusters in the Security Control Plane with metadata and cryptographic hashes of the file to enable further analysis. If unauthorized changes or anomalous connections are detected in the AWS infrastructure, an alert is generated from the Elasticsearch clusters to notify the Information Security team of an anomalous event.

2. For an on-premise Elasticsearch deployment, it is recommended that a third party HIDS/FIM be implemented as a risk reduction method for this control.

3. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes. For example, the Elasticsearch directory contents include among others:
LICENSE.txt, NOTICE.txt, README.asciidoc, bin, config, data, jdk, lib, logs, modules, plugins

References:

a. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
b. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting the integrity of the tools used for logging purposes is a critical step in ensuring the integrity of log data. Log data includes all information (e.g., log records, log settings, and log reports) needed to successfully log information system activity.

It is not uncommon for attackers to replace the log tools or inject code into the existing tools for the purpose of providing the capability to hide or erase system activity from the logs.

To address this risk, log tools must be cryptographically signed in order to provide the capability to identify when the log tools have been modified, manipulated or replaced. An example is a checksum hash of the file or files.

Application server log tools must use cryptographic mechanisms to protect the integrity of the tools or allow cryptographic protection mechanisms to be applied to their tools.

Legacy Ids: V-35445; SV-46732

Comments:

CCI: CCI-001496The information system implements cryptographic mechanisms to protect the integrity of audit tools.NIST SP 800-53 :: AU-9 (3)NIST SP 800-53A :: AU-9 (3).1NIST SP 800-53 Revision 4 :: AU-9 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must automatically terminate a user session after organization-defined conditions or trigger events requiring a session disconnect.
STIG ID: SRG-APP-000295 **Rule ID:** SV-204777r508029_rule **Vul ID:** V-204777
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server is configured to close user sessions after defined conditions or trigger events are met.

If the application server is not configured or cannot be configured to disconnect users after defined conditions and trigger events are met, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to support automatically disconnect a user session after organization-defined conditions or trigger events requiring session disconnect.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout

Sets the session duration. By default, sessions stay active until the browser is closed. When this is set to an explicit idle timeout, closing the browser still requires the user to log back into Kibana.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g., 70ms, 5s, 3d, 1Y).

xpack.security.session.lifespan

Sets the maximum duration, also known as "absolute timeout". By default, a session can be renewed indefinitely. When this value is set, a session will end once its lifespan is exceeded, even if the user is not idle. NOTE: if idleTimeout is not set, this setting will still cause sessions to expire.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html

e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
m. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: An attacker can take advantage of user sessions that are left open, thus bypassing the user authentication process.

To thwart the vulnerability of open and unused user sessions, the application server must be configured to close the sessions when a configured condition or trigger event is met.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

Legacy Ids: V-57401; SV-71673

Comments:

CCI: CCI-002361The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.NIST SP 800-53 Revision 4 :: AC-12

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server management interface must provide a logout capability for user-initiated communication session.
STIG ID: SRG-APP-000296 **Rule ID:** SV-204778r508029_rule **Vul ID:** V-204778
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server management interface provides a logout capability.

If the application server management interface does not provide a logout capability, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to provide a logout capability for user-initiated communication session.

2. Kibana logout and authentication settings are available at:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
Examples:
Local and global logout

During logout, both the Kibana session and Elasticsearch access/refresh token pair are invalidated. This is known as "local" logout.

Kibana can also initiate a "global" logout or Single Logout if it’s supported by the external authentication provider and not explicitly disabled by Elasticsearch. In this case, the user is redirected to the external authentication provider for log out of all applications associated with the active provider session.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If a user cannot explicitly end an application server management interface session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session.

The attacker will then have access to the application server management functions without going through the user authentication process.

To prevent this type of attack, the application server management interface must close user sessions when defined events are met and provide a logout function for users to explicitly close the session and free resources that were in use by the user.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or

a hybrid with another control provider.

Legacy Ids: V-57403; SV-71675

Comments:

CCI: CCI-002363The information system provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to organization-defined information resources.NIST SP 800-53 Revision 4 :: AC-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server management interface must display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.
STIG ID: SRG-APP-000297 **Rule ID:** SV-204779r508029_rule **Vul ID:** V-204779
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration settings to determine if the application server management interface displays a logout message.

If the application server management interface does not display a logout message, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. Kibana as the front end can be used, and Kibana will display a logout message - the feature is not configurable. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to display an explicit logout message to users indicating the reliable termination of authenticated sessions.

2. Kibana logout and authentication settings are available at:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html

Examples:
Local logout: During logout, both the Kibana session and Elasticsearch access/refresh token

pair are invalidated. This is known as "local" logout.

Global logout: Kibana can also initiate a "global" logout or Single Logout if it's supported by the external authentication provider and not explicitly disabled by Elasticsearch. In this case, the user is redirected to the external authentication provider for log out of all applications associated with the active provider session.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Providing a logout capability to the user allows the user to explicitly close a session and free those resources used during the session.

If a user cannot explicitly end an application session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session.

The attacker will then have access to the application server management functions without going through the user authentication process.

To inform the user that the session has been reliably closed, a logout message must be displayed to the user.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57405; SV-71677

Comments:

CCI: CCI-002364The information system displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.NIST SP 800-53 Revision 4 :: AC-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.
STIG ID: SRG-APP-000313 **Rule ID:** SV-204780r508029_rule **Vul ID:** V-204780
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation to determine if the application associates organization-defined types of security attributes with organization-defined security attribute values to information in process.

If the application server does not associate the security attributes to information in process or the feature is not implemented, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a particular format.

3. Logstash and or Beats should be configured to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

4. All applications logs/events should associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

5. Recommend using Elasticsearch index templates where possible.

6. In Elasticsearch, mapping is the description of how documents and the fields they contain are stored and indexed. In the mapping, define the following, for example:
- The structure of the document (fields and data type of those fields)
- How to transform values before indexing
- What fields use for full-text searching

7. Update the index mapping definitions as needed to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

References:

a. Mapping: https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping.html
b. Index Template:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-templates.html
c. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
d. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
e. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
f. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
g. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
h. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
i. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
j. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
k. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
l. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
m. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
n. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
o. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
p. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
q. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Install Elastic Agents :

https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server provides a framework for applications to communicate between each other to form an overall well-designed application to perform a task. As the information traverses the application server and the components, the security attributes must be maintained. Without the association of security attributes to information, there is no basis for the application server or hosted applications to make security-related access control decisions. The security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information.

One example includes marking data as classified or FOUO. These security attributes may be assigned manually or during data processing, but either way, it is imperative these assignments are maintained while the data is in process. If the security attributes are lost when the data is being processed, there is the risk of a data compromise.

Legacy Ids: V-57407; SV-71679

Comments:

CCI: CCI-002263The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.NIST SP 800-53 Revision 4 :: AC-16 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.
STIG ID: SRG-APP-000314 **Rule ID:** SV-204781r508029_rule **Vul ID:** V-204781
Severity: CAT II

Documentable: No

Check Content:

Review the application server documentation to determine if the application associates organization-defined types of security attributes with organization-defined security attribute values to information in transmission.

If the application server does not associate the security attributes to information in transmission or the feature is not implemented, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a particular format.

3. Logstash and/or Beats should be configured to associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.

4. All applications logs/events should associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.

5. Recommend using Elasticsearch index templates where possible.

6. In Elasticsearch, mapping is the description of how documents and the fields they contain are stored and indexed. In the mapping, you can define, for example, the following:
- The structure of the document (fields and data type of those fields)
- How to transform values before indexing
- What fields use for full-text searching

7. Update the index mapping definitions as needed to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.

References:

a. Mapping: https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping.html
b. Index Template:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-templates.html
c. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
d. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
e. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
f. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html

g. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
h. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
i. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
j. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
k. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
l. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
m. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
n. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
o. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
p. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
q. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
r. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The application server provides a framework for applications to communicate between each other to form an overall well-designed application to perform a task. As the information is transmitted, the security attributes must be maintained. Without the association of security attributes to information, there is no basis for the application to make security-related access control decisions.

Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information.

One example includes marking data as classified or FOUO. These security attributes may be assigned manually or during data processing, but either way, it is imperative these assignments are maintained while the data is in transmission. If the security attributes are lost when the data is being transmitted, there is the risk of a data compromise.

Legacy Ids: V-57409; SV-71681

Comments:

CCI: CCI-002264The organization provides the means to associate organization-defined

types of security attributes having organization-defined security attribute values with information in transmission.NIST SP 800-53 Revision 4 :: AC-16 a

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must control remote access methods.
STIG ID: SRG-APP-000315 **Rule ID:** SV-204782r508029_rule **Vul ID:** V-204782
Severity: CAT II

Documentable: No

Check Content:
Review organization policy, application server product documentation and configuration to determine if the system enforces the organization's requirements for remote connections.

If the system is not configured to enforce these requirements, or the remote connection settings are not in accordance with the requirements, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports mutual TLS for the HTTP layer. A proxy should be placed in front of the cluster to satisfy this control, which can be configured for mTLS with Elasticsearch to facilitate monitoring and control of web based or command line based administrative connections.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Application servers provide remote access capability and must be able to enforce remote access policy requirements or work in conjunction with enterprise tools designed to enforce policy requirements. Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by logging connection activities of remote users.

Examples of policy requirements include, but are not limited to, authorizing remote access to the information system, limiting access based on authentication credentials, and monitoring for unauthorized access.

Legacy Ids: V-57413; SV-71685

Comments:

CCI: CCI-002314The information system controls remote access methods.NIST SP 800-53 Revision 4 :: AC-17 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide the capability to immediately disconnect or disable remote access to the management interface.
STIG ID: SRG-APP-000316 **Rule ID:** SV-204783r508029_rule **Vul ID:** V-204783
Severity: CAT II

Documentable: No

Check Content:
Review the application server product documentation and server configuration to ensure that there is a capability to immediately disconnect or disable remote access to the management interface.

If there is no capability, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to immediately disconnect or disable remote access to the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without the ability to immediately disconnect or disable remote access, an attack or other compromise taking progress would not be immediately stopped.

The application server must have the capability to immediately disconnect current users remotely accessing the management interface and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57415; SV-71687

Comments:

CCI: CCI-002322The organization provides the capability to expeditiously disconnect or disable remote access to the information system within the organization-defined time period.NIST SP 800-53 Revision 4 :: AC-17 (9)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
STIG ID: SRG-APP-000340 **Rule ID:** SV-204784r508029_rule **Vul ID:** V-204784
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to verify that non-privileged users cannot access or execute privileged functions.

Have a user logon as a non-privileged user and attempt to execute privileged functions.

If the user is capable of executing privileged functions, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm.

2. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

3. Configure the Application Server to allow only the ISSM (or individuals or roles appointed by the ISSM) to the required privileges.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html

c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
i. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
j. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Restricting non-privileged users also prevents an attacker, who has gained access to a non-privileged account, from elevating privileges, creating accounts, and performing system checks and maintenance.

Legacy Ids: V-57399; SV-71671

Comments:

CCI: CCI-002235The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.NIST SP 800-53 Revision 4 :: AC-6 (10)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide access logging that ensures users who are granted a privileged role (or roles) have their privileged activity logged.
STIG ID: SRG-APP-000343 **Rule ID:** SV-204785r508029_rule **Vul ID:** V-204785
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and log configuration to verify the application server logs privileged activity.

If the application server is not configured to log privileged activity, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

Note: If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log privileged activity.

References:

a. Enabling audit logging:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/current/authorization.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/current/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/current/custom-realms.html
k. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
l. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
m. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: In order to be able to provide a forensic history of activity, the application server must ensure users who are granted a privileged role or those who utilize a separate distinct account when accessing privileged functions or data have their actions logged.

If privileged activity is not logged, no forensic logs can be used to establish accountability for privileged actions that occur on the system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57397; SV-71669

Comments:

CCI: CCI-002234The information system audits the execution of privileged functions.NIST SP 800-53 Revision 4 :: AC-6 (9)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide centralized management and configuration of the content to be captured in log records generated by all application components.
STIG ID: SRG-APP-000356 **Rule ID:** SV-204787r508029_rule **Vul ID:** V-204787
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server is part of a cluster.

If the application server is not part of a cluster, this requirement is NA.

If the application server is part of a cluster, verify that the log settings are managed and configured from a centralized management server.

If the log settings are not centrally managed, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch provides a clustering capability by design.

A single instance of Elasticsearch is a node. A collection of connected nodes is called a cluster.

Nodes are added to a cluster to increase its capacity and reliability. By default, a node is both a data node and eligible to be elected as the master node that controls the cluster. A node can be configured for a specific purpose, such as handling ingest requests.

2. Elasticsearch natively does not provide a GUI interface. Recommended to use the Kibana UI for centralized management and configuration of the content to be captured in log records generated by all application components.

Access to individual features is governed by Elasticsearch and Kibana privileges.

References:

a. Add and remove nodes in your cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-node.html
c. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A clustered application server is made up of several servers working together to provide the user a failover and increased computing capability. To facilitate uniform logging in the event of an incident and later forensic investigation, the record format and logable events need to be uniform. This can be managed best from a centralized server.

Without the ability to centrally manage the content captured in the log records, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

Legacy Ids: V-57419; SV-71691

Comments:

CCI: CCI-001844The information system provides centralized management and configuration of the content to be captured in audit records generated by organization-defined information system components.NIST SP 800-53 Revision 4 :: AU-3 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must allocate log record storage capacity in accordance with organization-defined log record storage requirements.
STIG ID: SRG-APP-000357 **Rule ID:** SV-204788r508029_rule **Vul ID:** V-204788
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server creates log storage to buffer log data until offloading to a log data storage facility.

If the application server does not allocate storage for log data, this is a finding.

Fix Text:
Steps/Recommendation:

1. Allocate sufficient audit storage space on each of the Elastic cluster nodes to support peak demand in accordance with organization-defined audit record storage requirements.

2. Recommend creating an immediate alert to the appropriate personnel (at a minimum) when allocated log record storage volume reaches a threshold of the repository maximum log record storage capacity.

3. Elasticsearch will go into a read-only state when it detects issues with disk storage which is the most common issue affecting logging. Elasticsearch will not shutdown if logging fails for other reasons.

4. Elasticsearch should be configured so as to continue to log but cache the logs locally until log shipment can resume.

5. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Returns information about a cluster's nodes.
Request
GET /_cat/nodes

disk.total, dt, diskTotal
Total disk space, such as 458.3gb.
disk.used, du, diskUsed
Used disk space, such as 259.8gb.
disk.avail, d, disk, diskAvail
Available disk space, such as 198.4gb.
disk.used_percent, dup, diskUsedPercent
Used disk space percentage, such as 47.

6. Kibana Alerts
The Elastic Stack monitoring features provide Kibana alerts out-of-the box to notify of potential issues in the Elastic Stack. These alerts are preconfigured based on the best practices recommended by Elastic. However, it can be tailored to meet organizational needs.

Disk usage threshold

This alert is triggered when a node is nearly at disk capacity. By default, the trigger condition is set at 80 percent or more averaged over the last 5 minutes. The alert is grouped across all the nodes of the cluster by running checks on a schedule time of 1 minute with a re-notify internal of 1 day.

References:

a. How monitoring works:
https://www.elastic.co/guide/en/elasticsearch/reference/current/how-monitoring-works.html
b. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/current/monitoring-overview.html
c. Kibana Alerts: https://www.elastic.co/guide/en/kibana/current/kibana-alerts.html
d. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/current/xpack-alerting.html
e. Monitor a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitor-elasticsearch-cluster.html
f. cat indices API: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-nodes.html
g. Alerting: https://www.elastic.co/guide/en/kibana/8.0/alerting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The proper management of log records not only dictates proper archiving processes and procedures be established, it also requires allocating enough storage space to maintain the logs online for a defined period of time.

If adequate online log storage capacity is not maintained, intrusion monitoring, security investigations, and forensic analysis can be negatively affected.

It is important to keep a defined amount of logs online and readily available for investigative purposes. The logs may be stored on the application server until they can be archived to a log system or, in some instances, a Storage Area Networks (SAN). Regardless of the method used, log record storage capacity must be sufficient to store log data when the data cannot be offloaded to a log system or SAN.

Legacy Ids: V-57421; SV-71693

Comments:

CCI: CCI-001849The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.NIST SP 800-53 Revision 4 :: AU-4

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must off-load log records onto a different system or media from the system being logged.
STIG ID: SRG-APP-000358 **Rule ID:** SV-204789r508029_rule **Vul ID:** V-204789
Severity: CAT II

Documentable: No

Check Content:
Verify the log records are being off-loaded to a separate system or transferred from the application server to a storage location other than the application server itself.

The system administrator of the device may demonstrate this capability using a log management application, system configuration, or other means.

If logs are not being off-loaded, this is a finding.

Fix Text:
Steps/Recommendation:

1. Setup appropriate lifecycle for the indices and create snapshots.

2. Elasticsearch can be configured to off-load log records onto a different system or media from the system being logged.

References:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/current/resiliency.html
b. Manage the index lifecycle:
https://www.elastic.co/guide/en/elasticsearch/reference/current/index-lifecycle-management.html
c. Automate snapshots with SLM:
https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshots-take-snapshot.html#automate-snapshots-slm

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, filenames involved, access control or flow control rules invoked.

Off-loading is a common process in information systems with limited log storage capacity.

Centralized management of log records provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records. Application servers and their related components are required to off-load log records onto a different system or media than the system being logged.

Legacy Ids: V-57423; SV-71695

Comments:

CCI: CCI-001851The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.NIST SP 800-53 Revision 4 :: AU-4 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide an immediate warning to the SA and ISSO, at a minimum, when allocated log record storage volume reaches 75% of maximum log record storage capacity.
STIG ID: SRG-APP-000359 **Rule ID:** SV-204790r508029_rule **Vul ID:** V-204790
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server logging system provides a warning to the SA and ISSO when 75% of allocated log record storage volume is reached.

If designated alerts are not sent, or the application server is not configured to use a dedicated logging tool that meets this requirement, this is a finding.

Fix Text:
Steps/Recommendation:

Recommend setting up an alert to the SA and ISSO, at a minimum, when allocated log record storage volume reaches 75% of maximum log record storage capacity.

1. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Recommend using Machine Learning to identify anomalies in an environment to reduce the manual steps required to create individual alerts.

3. Metricbeat is the recommended method for collecting and shipping monitoring data to a monitoring cluster.

4. After collecting monitoring data for one or more products in the Elastic Stack, Kibana can be configured to retrieve that information and display it in on the Stack Monitoring page.

5. At a minimum, capture monitoring data for the Elasticsearch production cluster. Once that data exists, Kibana can display monitoring data for other products in the cluster.

6. Identify where to retrieve monitoring data from. The cluster that contains the monitoring data is referred to as the monitoring cluster. If the monitoring data is stored on a dedicated monitoring cluster, it is accessible even when the cluster monitoring is not.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

7. By default, data is retrieved from the cluster specified in the elasticsearch.hosts value in the kibana.yml file.

8. If the Elastic security features are enabled on the monitoring cluster, configure a user ID and password so Kibana can retrieve the data.
- Create a user that has the monitoring_user built-in role on the monitoring cluster.
- Add the xpack.monitoring.elasticsearch.username and xpack.monitoring.elasticsearch.password settings in the kibana.yml file. If these settings are omitted, Kibana uses the elasticsearch.username and elasticsearch.password setting values.

9. If the Elastic security features are enabled on the Kibana server, only users that have the authority to access Kibana indices and to read the monitoring indices can use the monitoring dashboards.
- These users must exist on the monitoring cluster. When accessing a remote monitoring cluster, use credentials that are valid on both the Kibana server and the monitoring cluster.
- Create users that have the monitoring_user and kibana_admin built-in roles.

10. Open Kibana in your web browser.
By default, go to http://localhost:5601/.
If the Elastic security features are enabled, log in.

11. In the side navigation, click Stack Monitoring.
If data collection is disabled, a prompt will be displayed to turn on data collection. If Elasticsearch security features are enabled, manage cluster privileges are needed to turn on data collection.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Use the cat indices API to get the following information for each index in a cluster:
- Shard count
- Document count
- Deleted document count
- Primary store size
- Total store size of all shards, including shard replicas

These metrics are retrieved directly from Lucene, which Elasticsearch uses internally to power indexing and search. As a result, all document counts include hidden nested documents.

To get an accurate count of Elasticsearch documents, use the cat count or count APIs.

References:
a. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/configuring-monitoring.html
b. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/monitoring-data.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. cat indices API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process logs as required. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded.

Notification of the storage condition will allow administrators to take actions so that logs are not lost. This requirement can be met by configuring the application server to utilize a dedicated logging tool that meets this requirement.

Legacy Ids: V-57427; SV-71699

Comments:

CCI: CCI-001855The information system provides a warning to organization-defined personnel, roles, and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.NIST SP 800-53 Revision 4 :: AU-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must provide an immediate real-time alert to authorized users of all log failure events requiring real-time alerts.
STIG ID: SRG-APP-000360 **Rule ID:** SV-204791r508029_rule **Vul ID:** V-204791
Severity: CAT II

Documentable: No

Check Content:
Review the configuration settings to determine if the application server log system provides a real-time alert to authorized users when log failure events occur requiring real-time alerts.

If designated alerts are not sent to authorized users, this is a finding.

Fix Text:
Steps/Recommendation:

Recommend setting up an alert to the SA and ISSO, at a minimum, when allocated log record storage volume reaches 75% of maximum log record storage capacity.

1. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Recommend using Machine Learning to identify anomalies in an environment to reduce the manual steps required to create individual alerts.

3. Metricbeat is the recommended method for collecting and shipping monitoring data to a monitoring cluster.

4. After collecting monitoring data for one or more products in the Elastic Stack, Kibana can be configured to retrieve that information and display it in on the Stack Monitoring page.

5. At a minimum, capture monitoring data for the Elasticsearch production cluster. Once that data exists, Kibana can display monitoring data for other products in the cluster.

6. Identify where to retrieve monitoring data from. The cluster that contains the monitoring data is referred to as the monitoring cluster. If the monitoring data is stored on a dedicated monitoring cluster, it is accessible even when the cluster monitoring is not.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

7. By default, data is retrieved from the cluster specified in the elasticsearch.hosts value in the kibana.yml file.

8. If the Elastic security features are enabled on the monitoring cluster, configure a user ID and password so Kibana can retrieve the data.
- Create a user that has the monitoring_user built-in role on the monitoring cluster.
- Add the xpack.monitoring.elasticsearch.username and xpack.monitoring.elasticsearch.password settings in the kibana.yml file. If these settings are omitted, Kibana uses the elasticsearch.username and elasticsearch.password setting values.

9. If the Elastic security features are enabled on the Kibana server, only users that have the authority to access Kibana indices and to read the monitoring indices can use the monitoring dashboards.
- These users must exist on the monitoring cluster. When accessing a remote monitoring cluster, use credentials that are valid on both the Kibana server and the monitoring cluster.
- Create users that have the monitoring_user and kibana_admin built-in roles.

10. Open Kibana in your web browser.
By default, go to http://localhost:5601/.
If the Elastic security features are enabled, log in.

11. In the side navigation, click Stack Monitoring.
If data collection is disabled, a prompt will be displayed to turn on data collection. If Elasticsearch security features are enabled, manage cluster privileges are needed to turn on data collection.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Use the cat indices API to get the following information for each index in a cluster:
- Shard count
- Document count
- Deleted document count
- Primary store size
- Total store size of all shards, including shard replicas

These metrics are retrieved directly from Lucene, which Elasticsearch uses internally to power indexing and search. As a result, all document counts include hidden nested documents.

To get an accurate count of Elasticsearch documents, use the cat count or count APIs.

References:

a. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/configuring-monitoring.html
b. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/monitoring-data.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. cat indices API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process logs as required. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. Notification of the failure event will allow administrators to take actions so that logs are not lost.

Legacy Ids: V-57429; SV-71701

Comments:

CCI: CCI-001858The information system provides a real-time alert in organization-defined real-time period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.NIST SP 800-53 Revision 4 :: AU-5 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must compare internal application server clocks at least every 24 hours with an authoritative time source.
STIG ID: SRG-APP-000371 **Rule ID:** SV-204792r508029_rule **Vul ID:** V-204792
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and confirm that the application server compares internal application server clocks at least every 24 hours with an authoritative time source.

If the application server does not compare internal application server clocks to an authoritative source or if the frequency is greater than every 24 hours, this is a finding.

Fix Text:
Stp/3Recommendation:

1. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index.

```
date {
match =>; ...
time zone =>; "%{tz}"; # or the defined field name
}
```

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/master/add-locale.html
c. Ingest processor reference:
https://www.elastic.co/guide/en/elasticsearch/reference/master/processors.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronization of system clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. To meet this requirement, the organization will define an authoritative time source and have each system compare its internal clock at least every 24 hours.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57435; SV-71707

Comments:

CCI: CCI-001891The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must synchronize internal application server clocks to an authoritative time source when the time difference is greater than the organization-defined time period.
STIG ID: SRG-APP-000372 **Rule ID:** SV-204793r508029_rule **Vul ID:** V-204793
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server is configured to reset internal information clocks when the difference is greater than a defined threshold with an authoritative time source.

If the application server cannot synchronize internal application server clocks to the authoritative time source when the time difference is greater than the organization-defined time period, this is a finding.

Fix Text:
Step/Recommendation:

1. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index.

```
date {
match =>; ...
time zone =>; "%{tz}"; # or the defined field name
}
```

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/master/add-locale.html
c. Ingest processor reference:
https://www.elastic.co/guide/en/elasticsearch/reference/master/processors.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronization of internal application server clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. To meet this requirement, the organization will define an authoritative time source and have each system synchronize when the time difference is greater than a defined time period. The industry standard for the threshold is 1ms.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or

a hybrid with another control provider.

Legacy Ids: V-57437; SV-71709

Comments:

CCI: CCI-002046The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.NIST SP 800-53 Revision 4 :: AU-8 (1) (b)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must record time stamps for log records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).
STIG ID: SRG-APP-000374 **Rule ID:** SV-204794r508029_rule **Vul ID:** V-204794
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration files to determine if time stamps for log records can be mapped to UTC or GMT.

If the time stamp cannot be mapped to UTC or GMT, this is a finding.

Fix Text:
Steps/Recommendation:

Elasticsearch architecture is designed to collect log records from multiple components within the server into a system-wide log trail.

1. All applications should capture the time of log/event creation.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Setup all the host/device to use UTC time zone (or GMT as per the business requirement), use NTP/Chrony to avoid time drift and be time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail. Also, use beat/Logstash to have time enabled in all index.

date {
match =>; ...

time zone =>; "%{tz}"; # or the defined field name
}

4. To verify if the ingest pipeline is setup to capture the time, use the following: GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/master/add-locale.html
c. Ingestor processor reference:
https://www.elastic.co/guide/en/elasticsearch/reference/master/processors.html
d. Ingest node: https://www.elastic.co/guide/en/elasticsearch/reference/master/ingest.html
e. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/master/date-processor.html
f. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/master/get-pipeline-api.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the application include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57431; SV-71703

Comments:

CCI: CCI-001890The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).NIST SP 800-53 Revision 4 :: AU-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must record time stamps for log records that meet a granularity of one second for a minimum degree of precision.
STIG ID: SRG-APP-000375 **Rule ID:** SV-204795r508029_rule **Vul ID:** V-204795
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration files to determine if time stamps for log records meet a granularity of one second.

If the time stamp cannot generate to a one-second granularity, this is a finding.

Fix Text:
Steps/Recommendation:

1. In JSON, dates are represented as strings. Elasticsearch uses a set of preconfigured formats to recognize and parse these strings into a long value representing milliseconds-since-the-epoch in UTC.

2. Elastic Stack's UI (Kibana) can also be utilized to search records that meet a granularity of one second for a minimum degree of precision.

Reference:

a. Mapping date format:
https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-date-format.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To investigate an incident, the log records should be easily put into chronological order. Without sufficient granularity of time stamps, the chronological order cannot be determined.

Time stamps generated by the application server include date and time. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks.

Legacy Ids: V-57433; SV-71705

Comments:

CCI: CCI-001889The information system records time stamps for audit records that meets organization-defined granularity of time measurement.NIST SP 800-53 Revision 4 :: AU-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must enforce access restrictions associated with changes to application server configuration.
STIG ID: SRG-APP-000380 **Rule ID:** SV-204796r508029_rule **Vul ID:** V-204796
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the system employs mechanisms to enforce restrictions on application server configuration changes.

Configuration changes include, but are not limited to, automatic code deployments, software library updates, and changes to configuration settings within the application server.

If the application server does not enforce access restrictions for configuration changes, this is a finding.

Fix Text:
Steps/Recommendation:

1.For on-premises implementation, the Elasticsearch system does not prevent modifications on the software resident within software libraries.

Configure the application OS file permissions to enforce access restrictions associated with changes to the application server configuration to include code deployment, library updates, and changes to application server configuration settings.

2. For the hosted Elasticsearch Service (SaaS offering), only an Elastic Admin with access to the Infrastructure as Code files would be able to modify files and modules that cannot be configured directly by the Customer. The Customer is responsible for a secure configuration

with Role-based access control (RBAC) controls. Elastic monitors for such changes in the hosted production environment and investigates if detected.

Reference:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When dealing with access restrictions pertaining to change control, it should be noted that any changes to the software, and/or application server configuration can potentially have significant effects on the overall security of the system.

Access restrictions for changes also include application software libraries.

If the application server provides automatic code deployment capability, (where updates to applications hosted on the application server are automatically performed, usually by the developers' IDE tool), it must also provide a capability to restrict the use of automatic application deployment. Automatic code deployments are allowable in a development environment, but not in production.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57491; SV-71767

Comments:

CCI: CCI-001813The information system enforces access restrictions.NIST SP 800-53 Revision 4 :: CM-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must log the enforcement actions used to restrict access associated with changes to the application server.

STIG ID: SRG-APP-000381 **Rule ID:** SV-204797r508029_rule **Vul ID:** V-204797
Severity: CAT II

Documentable: No

Check Content:
Check the application server documentation and logs to determine if enforcement actions used to restrict access associated with changes to the application server are logged.

If these actions are not logged, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, configure the application OS to log the enforcement actions used to restrict access associated with changes to the application server filesystem.

2. For the hosted Elasticsearch Service (SaaS offering), only an Elastic Admin with access to the Infrastructure as Code files would be able to modify files and modules that cannot be configured directly by Customer. Customer is responsible for secure configuration with Role-based access control (RBAC) controls. Elastic monitors for such changes in the hosted production environment and investigates if detected.

3. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

Note: If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

4. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

5. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers to log the enforcement actions used to restrict access associated with changes to the application server

fiesystem.

6. Configure the application OS file permissions to restrict access to logs with least privilege permissions to only authorized users or processes. For example, the Elasticsearch directory contents include among others:

LICENSE.txt, NOTICE.txt, README.asciidoc, bin, config, data, jdk, lib, logs, modules, plugins

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/8.0/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
l. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n.Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without logging the enforcement of access restrictions against changes to the application server configuration, it will be difficult to identify attempted attacks, and a log trail will not be available for forensic investigation for after-the-fact actions. Configuration changes may occur to any of the modules within the application server through the management interface, but logging of actions to the configuration of a module outside the application server is not logged.

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. Enforcement action methods may be as simple as denying access to a file based on the application of file permissions (access restriction). Log items may consist of lists of actions blocked by access restrictions or changes identified after the fact.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57493; SV-71769

Comments:

CCI: CCI-001814The Information system supports auditing of the enforcement actions.NIST SP 800-53 Revision 4 :: CM-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must require users to re-authenticate when organization-defined circumstances or situations require re-authentication.
STIG ID: SRG-APP-000389 **Rule ID:** SV-204798r508029_rule **Vul ID:** V-204798
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server requires a user to re-authenticate when organization-defined circumstances or situations are met.

If the application server does not require a user to re-authenticate when organization-defined

circumstances or situations are met, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to require a user to re-authenticate when organization-defined circumstances or situations are met.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout

Ensures that user sessions will expire after a period of inactivity. This and xpack.security.session.lifespan are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.lifespan

Ensures that user sessions will expire after the defined time period. This behavior is also known as an "absolute timeout". If this is not set, user sessions could stay active indefinitely. This and xpack.security.session.idleTimeout are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.cleanupInterval

Sets the interval at which Kibana tries to remove expired and invalid sessions from the session index. By default, this value is 1 hour. The minimum value is 10 seconds.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When applications provide the capability to change security roles or escalate the functional capability of the application, it is critical the user re-authenticate.

In addition to the re-authentication requirements associated with session locks, the application server security model may require re-authentication of individuals in other situations, including (but not limited to) the following circumstances:

(i) When authenticators change;
(ii) When roles change;
(iii) When security categories of information systems change;
(iv) When the execution of privileged functions occurs;
(v) After a fixed period of time; or
(vi) Periodically.

Within the DoD, the minimum circumstances requiring re-authentication are privilege escalation and role changes.

Organization is responsible for satisfying all the security controls for the external

dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57523; SV-71799

Comments:

CCI: CCI-002038The organization requires users to reauthenticate when organization-defined circumstances or situations requiring reauthentication.NIST SP 800-53 Revision 4 :: IA-11

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must require devices to re-authenticate when organization-defined circumstances or situations require re-authentication.
STIG ID: SRG-APP-000390 **Rule ID:** SV-204799r508029_rule **Vul ID:** V-204799
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server requires devices to re-authenticate when organization-defined circumstances or situations require re-authentication.

If the application server does not require a device to re-authenticate, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch itself does not provide session control. Kibana can be used as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to require devices to re-authenticate when organization-defined circumstances or situations are met.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout

Ensures that user sessions will expire after a period of inactivity. This and xpack.security.session.lifespan are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.lifespan

Ensures that user sessions will expire after the defined time period. This behavior also known as an "absolute timeout". If this is not set, user sessions could stay active indefinitely. This and xpack.security.session.idleTimeout are both highly recommended. By default, this setting is not set.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 20m, 24h, 7d, 1w).

xpack.security.session.cleanupInterval

Sets the interval at which Kibana tries to remove expired and invalid sessions from the session index. By default, this value is 1 hour. The minimum value is 10 seconds.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g., 20m, 24h, 7d, 1w).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without re-authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of devices, including (but not limited to), the following other situations.

(i) When authenticators change;
(ii) When roles change;
(iii) When security categories of information systems change;
(iv) After a fixed period of time; or
(v) Periodically.

For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification decisions (as opposed to the actual identifiers) to the services that need to act on those decisions.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57525; SV-71801

Comments:

CCI: CCI-002039The organization requires devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.NIST SP 800-53 Revision 4 :: IA-11

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must accept Personal Identity Verification (PIV) credentials to access the management interface.
STIG ID: SRG-APP-000391 **Rule ID:** SV-204800r508029_rule **Vul ID:** V-204800

Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to ensure the application server accepts PIV credentials to the management interface.

If PIV credentials are not accepted, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides Personal Identity Verification (PIV) credentials to access the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

PIV credentials are only used in an unclassified environment.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12, as well as its use as a primary component of layered protection for national security systems.

The application server must support the use of PIV credentials to access the management interface and perform management functions.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57503; SV-71779

Comments:

CCI: CCI-001953The information system accepts Personal Identity Verification (PIV) credentials.NIST SP 800-53 Revision 4 :: IA-2 (12)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must electronically verify Personal Identity Verification (PIV) credentials for access to the management interface.
STIG ID: SRG-APP-000392 **Rule ID:** SV-204801r508029_rule **Vul ID:** V-204801
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to ensure the application server electronically verifies PIV credentials to the management interface.

If PIV credentials are not electronically verified, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which must electronically verify Personal Identity Verification (PIV) credentials for access to the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The use of Personal Identity Verification (PIV) credentials facilitates standardization and reduces the risk of unauthorized access.

PIV credentials are only used in an unclassified environment.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12, as well as its use as a primary component of layered protection for national security systems.

The application server must electronically verify the use of PIV credentials to access the management interface and perform management functions.

Organization is responsible for satisfying all the security controls for the external

dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57505; SV-71781

Comments:

CCI: CCI-001954The information system electronically verifies Personal Identity Verification (PIV) credentials.NIST SP 800-53 Revision 4 :: IA-2 (12)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must prohibit the use of cached authenticators after an organization-defined time period.
STIG ID: SRG-APP-000400 **Rule ID:** SV-204804r508029_rule **Vul ID:** V-204804
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server prohibits the use of cached authenticators after an organization-defined timeframe.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and authenticate users. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which prohibit the use of cached authenticators after an organization-defined time period.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html

d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When the application server is using PKI authentication, a local revocation cache must be stored for instances when the revocation cannot be authenticated through the network, but if cached authentication information is out of date, the validity of the authentication information may be questionable.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57513; SV-71789

Comments:

CCI: CCI-002007The information system prohibits the use of cached authenticators after an organization defined time period.NIST SP 800-53 Revision 4 :: IA-5 (13)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to

access revocation information via the network.
STIG ID: SRG-APP-000401 **Rule ID:** SV-204805r508029_rule **Vul ID:** V-204805
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to ensure the application server provides a PKI integration capability that implements a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.

If the application server is not configured to meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) that implements a local cache of revocation data to support path discovery and validation to manage accounts and authenticate users. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides multi-factor authentication. The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. OpenID Connect Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The cornerstone of the PKI is the private key used to encrypt or digitally sign information. The key by itself is a cryptographic value that does not contain specific user information.

Application servers must provide the capability to utilize and meet requirements of the DoD Enterprise PKI infrastructure for application authentication, but without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates) when access through the network to the CA is not available.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57511; SV-71787

Comments:

CCI: CCI-001991The information system for PKI-based authentication implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.NIST SP 800-53 Revision 4 :: IA-5 (2) (d)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must accept Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.
STIG ID: SRG-APP-000402 **Rule ID:** SV-204806r508029_rule **Vul ID:** V-204806
Severity: CAT II

Documentable: No

Check Content:

Review the application server documentation and configuration to determine if the application server accepts PIV credentials from other federal agencies to access the management interface.

If the application server does not accept other federal agency PIV credentials to access the management interface, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. PIV credentials are only used in an unclassified environment.

Access may be denied to authorized users if federal agency PIV credentials are not accepted to access the management interface.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57515; SV-71791

Comments:

CCI: CCI-002009The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.NIST SP 800-53 Revision 4 :: IA-8 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.
STIG ID: SRG-APP-000403 **Rule ID:** SV-204807r508029_rule **Vul ID:** V-204807
Severity: CAT II

Documentable: No

Check Content:
The CAC is the standard DoD authentication token;the PIV is the standard authentication token used by federal/civilian agencies.

If access to the application server is limited to DoD personnel accessing the system via CAC; and PIV access is not warranted or allowed as per the system security plan, the PIV requirement is NA.

Review the application server documentation and configuration to determine if the application server electronically verifies PIV credentials from other federal agencies to access the management interface.

If the application server does not electronically verify other federal agency PIV credentials to access the management interface, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies to access the management interface.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. PIV credentials are only used in an unclassified environment.

If PIV credentials are not electronically verified before accessing the management interface, unauthorized users may gain access to the system and data the user has not been granted access to.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57517; SV-71793

Comments:

CCI: CCI-002010The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.NIST SP 800-53 Revision 4 :: IA-8 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must accept FICAM-approved third-party credentials.
STIG ID: SRG-APP-000404 **Rule ID:** SV-204808r508029_rule **Vul ID:** V-204808
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server accepts FICAM-approved third-party credentials.

If the application server does not accept FICAM-approved third-party credentials, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

2. The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users. When using an IdP, Elasticsearch supports Federal Identity, Credential, and Access Management (FICAM) issued profiles such as SAML 2.0 and OpenID 2.0.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
j. Federal Identity, Credential, and Access Management Architecture:
https://arch.idmanagement.gov/
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Access may be denied to legitimate users if FICAM-approved third-party credentials are not accepted.

This requirement typically applies to organizational information systems that are accessible to non-federal government agencies and other partners. This allows federal government relying parties to trust such credentials at their approved assurance levels.

Third-party credentials are those credentials issued by non-federal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57519; SV-71795

Comments:

CCI: CCI-002011The information system accepts FICAM-approved third-party credentials.NIST SP 800-53 Revision 4 :: IA-8 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must conform to FICAM-issued profiles.
STIG ID: SRG-APP-000405 **Rule ID:** SV-204809r508029_rule **Vul ID:** V-204809
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server conforms to FICAM-issued profiles.

If the application server does not conform to FICAM-issued profiles, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to authenticate users.

2. The recommendation is to integrate Elasticsearch with an Identity Providers (IdP) to uniquely identify and authenticate users. When using an IdP, Elasticsearch supports Federal Identity, Credential, and Access Management (FICAM) issued profiles such as SAML 2.0 and OpenID 2.0.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
c. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. Elasticsearch Service - Hosted Elastic Stack:
https://www.elastic.co/guide/en/cloud/current/index.html
j. Federal Identity, Credential, and Access Management Architecture:
https://arch.idmanagement.gov/
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without conforming to FICAM-issued profiles, the information system may not be interoperable with FICAM-authentication protocols, such as SAML 2.0 and OpenID 2.0.

This requirement addresses open identity management standards.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57521; SV-71797

Comments:

CCI: CCI-002014The information system conforms to FICAM-issued profiles.NIST SP 800-53 Revision 4 :: IA-8 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions.
STIG ID: SRG-APP-000427 **Rule ID:** SV-204811r508029_rule **Vul ID:** V-204811
Severity: CAT II

Documentable: No

Check Content:

Review the application server documentation and configuration to determine if the application server only allows the use of DoD PKI-established certificate authorities.

If the application server allows other certificate authorities for verification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
q. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates. The application server must only allow the use of DoD PKI-established certificate authorities for verification.

Legacy Ids: V-57551; SV-71827

Comments:

CCI: CCI-002470The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.NIST SP 800-53 Revision 4 :: SC-23 (5)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.
STIG ID: SRG-APP-000428 **Rule ID:** SV-204812r508029_rule **Vul ID:** V-204812
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.

If the application server does not implement cryptographic mechanisms to prevent unauthorized modification, this is a finding.

Fix Text:

Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations: https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an application server. Alternative physical protection measures include protected distribution systems.

In order to prevent unauthorized disclosure or modification of the information, application servers must protect data at rest by using cryptographic mechanisms.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Legacy Ids: V-57557; SV-71833

Comments:

CCI: CCI-002475The information system implements cryptographic mechanisms to prevent

unauthorized modification of organization-defined information at rest on organization-defined information system components.NIST SP 800-53 Revision 4 :: SC-28 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application must implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.
STIG ID: SRG-APP-000429 **Rule ID:** SV-204813r508029_rule **Vul ID:** V-204813
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.

If the application server does not implement cryptographic mechanisms to prevent unauthorized disclosure, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Cloud Enterprise implements encryption at rest (EAR) by default. Elasticsearch Service supports EAR for both the data stored in clusters and the snapshots taken for backup, on all cloud platforms and across all regions.

2. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

3. Configure the application OS file permissions to restrict access to logs with the least privilege permissions to only authorized users or processes.

References:

a. Start the Elastic Stack with security enabled:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/3.0/ece-securing-considerations.html
c. Technical FAQ: https://www.elastic.co/guide/en/cloud/current/ec-faq-technical.html
d. Support Matrix: https://www.elastic.co/support/matrix

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an application server. Alternative physical protection measures include protected distribution systems.

In order to prevent unauthorized disclosure or modification of the information, application servers must protect data at rest by using cryptographic mechanisms.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57559; SV-71835

Comments:

CCI: CCI-002476The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.NIST SP 800-53 Revision 4 :: SC-28 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server, when a MAC I system, must be in a high-availability (HA) cluster.
STIG ID: SRG-APP-000435 **Rule ID:** SV-204814r508029_rule **Vul ID:** V-204814
Severity: CAT II

Documentable: No

Check Content:
If the application server is not a MAC I system, this requirement is NA.

Review the application server documentation and configuration to determine if the application server is part of an HA cluster.

If the application server is not part of an HA cluster, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch provides a clustering capability by design and can be configured in a high-availability (HA) cluster. Elasticsearch offers a number of features to achieve HA despite failures.

- With proper planning, a cluster can be designed for resilience to many of the things that commonly go wrong, from the loss of a single node or network connection right up to a zone-wide outage such as power loss.
- Enable cross-cluster replication to replicate data to a remote follower cluster which may be in a different data centre or even on a different continent from the leader cluster. The follower cluster acts as a hot standby, ready to fail over in the event of a disaster so severe that the leader cluster fails. The follower cluster can also act as a geo-replica to serve searches from nearby clients.
- The last line of defense against data loss is to take regular snapshots of the cluster so that a copy can be restored elsewhere if needed.

Designing for resilience
A resilient cluster requires redundancy for every required cluster component. This means a resilient cluster must have:
- At least three master-eligible nodes
- At least two nodes of each role
- At least two copies of each shard (one primary and one or more replicas)

Back up a cluster
WARNING: An Elasticsearch cluster cannot be backed up simply by copying the data directories of all of its nodes. Elasticsearch may be making changes to the contents of its data directories while it is running; copying its data directories cannot be expected to capture a consistent picture of their contents. If restoring a cluster from such a backup, it may fail and report corruption and/or missing files. Alternatively, it may appear to have succeeded though it silently lost some of its data. The only reliable way to back up a cluster is by using the snapshot and restore functionality.

To have a complete backup for a cluster:
- Back up the data
- Back up the cluster configuration
- Back up the security configuration

2. If using Elasticsearch as a SaaS product (Elastic-hosted), recommend a minimum of three availability zones to enable Elastic Cloud Enterprise to create clusters with a tiebreaker.

High availability
- Fault tolerance for Elastic Cloud Enterprise is based around the concept of availability

zones.
- An availability zone contains resources available to an Elastic Cloud Enterprise installation that are isolated from other availability zones to safeguard against potential failure.
- If there are only two availability zones in total in the installation, no tiebreaker is created.

3. Refer to the cloud provider options of Regions and Availability Zones for high-availability (HA) cluster for hosting the Elastic cluster.

References:

a. Add and remove nodes in a cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/current/add-elasticsearch-nodes.html
b. Node: https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-node.html
c. Set up a cluster for high availability:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability.html
d. Designing for resilience:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/high-availability-cluster-design.html
e. Cross-cluster replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html
f. Create a snapshot:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/snapshots-take-snapshot.html
g. High availability: https://www.elastic.co/guide/en/cloud-enterprise/current/ece-ha.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A MAC I system is a system that handles data vital to the organization's operational readiness or effectiveness of deployed or contingency forces. A MAC I system must maintain the highest level of integrity and availability. By HA clustering the application server, the hosted application and data are given a platform that is load-balanced and provided high-availability.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57531; SV-71807

Comments:

CCI: CCI-002385The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.NIST SP 800-53 Revision 4 :: SC-5

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect against or limit the effects of all types of Denial of Service (DoS) attacks by employing organization-defined security safeguards.
STIG ID: SRG-APP-000435 **Rule ID:** SV-204815r508029_rule **Vul ID:** V-204815
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server can protect against or limit the effects of all types of Denial of Service (DoS) attacks by employing defined security safeguards.

If the application server cannot be configured to protect against or limit the effects of all types of DoS, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Stack does not have any built in Denial of Service (DoS) capability, therefore it is recommended to leverage a third-party Host Intrusion Detection System (HIDS) or Host Intrusion Prevention System (HIPS).

2. The HIDS or HIPS application should be installed, configured, and updated on each application server.

Note: A HIDS or HIPS application is a secondary line of defense behind the antivirus. The application will monitor all ports and the dynamic state of a development system. If the application detects irregularities on the system, it will block incoming traffic that may potentially compromise the development system that can lead to a DoS or data theft.

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity. To reduce the possibility or effect of a DoS, the application server must employ defined security safeguards. These safeguards will be determined by the placement of the application server and the type of applications being hosted within the application server framework.

There are many examples of technologies that exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the application opens at one time). Employing increased capacity and bandwidth, combined with service redundancy or clustering, may reduce the susceptibility to some DoS attacks.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57529; SV-71805

Comments:

CCI: CCI-002385The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.NIST SP 800-53 Revision 4 :: SC-5

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must protect the confidentiality and integrity of transmitted information through the use of an approved TLS version.
STIG ID: SRG-APP-000439 **Rule ID:** SV-204816r508029_rule **Vul ID:** V-204816
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine which version of TLS is being used.

If the application server is not using TLS to maintain the confidentiality and integrity of transmitted information or non-FIPS-approved SSL versions are enabled, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html

g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Preventing the disclosure of transmitted information requires that the application server take measures to employ some form of cryptographic mechanism in order to protect the information during transmission. This is usually achieved through the use of Transport Layer Security (TLS).

Transmission of data can take place between the application server and a large number of devices/applications external to the application server. Examples are a web client used by a user, a backend database, a log server, or other application servers in an application server cluster.

If data is transmitted unencrypted, the data then becomes vulnerable to disclosure. The disclosure may reveal user identifier/password combinations, website code revealing business logic, or other user personal information.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-57533; SV-71809

Comments:

CCI: CCI-002418The information system protects the confidentiality and/or integrity of transmitted information.NIST SP 800-53 Revision 4 :: SC-8

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must remove all export ciphers to protect the confidentiality and integrity of transmitted information.
STIG ID: SRG-APP-000439 **Rule ID:** SV-204817r508029_rule **Vul ID:** V-204817
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine if export ciphers are removed.

If the application server does not have the export ciphers removed, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html

m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: During the initial setup of a Transport Layer Security (TLS) connection to the application server, the client sends a list of supported cipher suites in order of preference. The application server will reply with the cipher suite it will use for communication from the client list. If an attacker can intercept the submission of cipher suites to the application server and place, as the preferred cipher suite, a weak export suite, the encryption used for the session becomes easy for the attacker to break, often within minutes to hours.

Legacy Ids: V-61351; SV-75833

Comments:

CCI: CCI-002418The information system protects the confidentiality and/or integrity of transmitted information.NIST SP 800-53 Revision 4 :: SC-8

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must employ approved cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

STIG ID: SRG-APP-000440 **Rule ID:** SV-204818r508029_rule **Vul ID:** V-204818
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation and configuration to determine if the application server employs approved cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

If the application server does not employ approved cryptographic mechanisms, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Preventing the disclosure or modification of transmitted information requires that application servers take measures to employ approved cryptography in order to protect the information during transmission over the network. This is usually achieved through the use of Transport Layer Security (TLS), SSL VPN, or IPSec tunnel.

If data in transit is unencrypted, it is vulnerable to disclosure and modification. If approved cryptographic algorithms are not used, encryption strength cannot be assured.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Legacy Ids: V-57535; SV-71811

Comments:

CCI: CCI-002421The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards.NIST SP 800-53 Revision 4 :: SC-8 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must maintain the confidentiality and integrity of information during preparation for transmission.
STIG ID: SRG-APP-000441 **Rule ID:** SV-204819r508029_rule **Vul ID:** V-204819
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and deployed configuration to determine if the application server maintains the confidentiality and integrity of information during preparation before transmission.

If the confidentiality and integrity is not maintained, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html

h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

An example of this would be an SMTP queue. This queue may be part of the application server so error messages from the server can be sent to system administrators, or SMTP functionality can be added to hosted applications by developers.

Any modules used by the application server that queue data before transmission must maintain the confidentiality and integrity of the information before the data is transmitted.

Legacy Ids: V-57537; SV-71813

Comments:

CCI: CCI-002420The information system maintains the confidentiality and/or integrity of information during preparation for transmission.NIST SP 800-53 Revision 4 :: SC-8 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must maintain the confidentiality and integrity of information during reception.
STIG ID: SRG-APP-000442 **Rule ID:** SV-204820r508029_rule **Vul ID:** V-204820
Severity: CAT II

Documentable: No

Check Content:
Review application server configuration to determine if the server is using a transmission method that maintains the confidentiality and integrity of information during reception.

If a transmission method is not being used that maintains the confidentiality and integrity of the data during reception, this is a finding.

Fix Text:
Steps/Recommendation:

Configure the Elasticsearch to maintain the confidentiality and integrity of information during preparation for transmission by configuring SSL/TLS encryption as well as encryption at rest of data stored in the Elastic cluster.

1. Enable Authentication and Authorization

2. Enable SSL/TLS encryption

3. Enable IP filtering

4. Disable anonymous user access to Elasticsearch if enabled.

Note: Incoming requests are considered to be anonymous if no authentication token can be extracted from the incoming request. By default, anonymous requests are rejected and an authentication error is returned (status code 401).

5. In elasticsearch.yml set
xpack.security.enabled: true
xpack.security.fips_mode.enabled: true

To enable encryption, you need to perform the following steps on each node in the cluster:

a. Generate a private key and X.509 certificate for each of your Elasticsearch nodes. See Generating Node Certificates.
b. Configure each node in the cluster to identify itself using its signed certificate and enable TLS on the transport layer. You can also optionally enable TLS on the HTTP layer. See Encrypting communications between nodes in a cluster and Encrypting HTTP client communications.
c. Configure the monitoring features to use encrypted connections. See Monitoring and security.
d. Configure Kibana to encrypt communications between the browser and the Kibana server and to connect to Elasticsearch via HTTPS. See Configuring security in Kibana.
e. Configure Logstash to use TLS encryption. See Configuring security in Logstash.
f. Configure Beats to use encrypted connections. For example, see Configure Filebeat to use security features.
g. Configure the Java transport client to use encrypted communications. See Java Client and security.
h. Configure Elasticsearch for Apache Hadoop to use secured transport. See Elasticsearch for Apache Hadoop Security.

6. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application servers with Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography).

7. Elastic Cloud Enterprise does not implement encryption at rest out of the box. To ensure encryption at rest for all data managed by Elastic Cloud Enterprise, the hosts running Elastic Cloud Enterprise must be configured with disk-level encryption, such as dm-crypt. In addition, snapshot targets must ensure that data is encrypted at rest as well.

8. Encryption at rest for Elasticsearch via dm-crypt is supported on all Linux OSs.

References:

a. Configuring Security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-security.html
b. Encrypting communications in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
c. Setting Up TLS on a Cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ssl-tls.html
d. FIPS-140-2:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
i. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
j. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
k. Configuring kibana:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Working with certificates:
https://www.elastic.co/guide/en/elasticsearch/client/net-api/8.0/working-with-certificates.html
p. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
q. Security considerations:
https://www.elastic.co/guide/en/cloud-enterprise/current/ece-securing-considerations.html
r. Support Matrix: https://www.elastic.co/support/matrix
s. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information can be either unintentionally or maliciously disclosed or modified during reception, including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Protecting the confidentiality and integrity of received information requires that application

servers take measures to employ approved cryptography in order to protect the information during transmission over the network. This is usually achieved through the use of Transport Layer Security (TLS), SSL VPN, or IPSEC tunnel.

The application server must utilize approved encryption when receiving transmitted data.

Legacy Ids: V-57539; SV-71815

Comments:

CCI: CCI-002422The information system maintains the confidentiality and/or integrity of information during reception.NIST SP 800-53 Revision 4 :: SC-8 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.
STIG ID: SRG-APP-000447 **Rule ID:** SV-204821r508029_rule **Vul ID:** V-204821
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the management interface behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

If the application server does not meet this requirement, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommended using the Kibana UI to manage the Elastic Stack and that Kibana performs input validation checks. Access to individual features is governed by Elasticsearch and Kibana privileges.

References:

a. Stack Management: https://www.elastic.co/guide/en/kibana/8.0/management.html
b. Security best practices:
https://www.elastic.co/guide/en/kibana/8.0/security-best-practices.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Invalid user input occurs when a user inserts data or characters into an applications data entry field and the application is unprepared to process that data. This results in unanticipated application behavior potentially leading to an application or information system compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

Application servers must ensure their management interfaces perform data input validation checks. When invalid data is entered, the application server must behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received. An example of a predictable behavior is trapping the data, logging the invalid data for forensic analysis if necessary, and continuing operation in a safe and secure manner.

Legacy Ids: V-57565; SV-71841

Comments:

CCI: CCI-002754The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.NIST SP 800-53 Revision 4 :: SI-10 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must remove organization-defined software components after updated versions have been installed.
STIG ID: SRG-APP-000454 **Rule ID:** SV-204822r508029_rule **Vul ID:** V-204822
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if organization-defined software components are removed after updated versions have been installed.

If organization-defined software components are not removed after updated versions have been installed, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, review all the nodes of the cluster to remove organization-defined software components after updated versions have been installed.

2. As part of the hosted Elasticsearch Service offering, review all the nodes of the cluster to remove organization-defined software components after updated versions have been installed.

ECE supports rolling upgrades on an Elasticsearch cluster to be upgraded one node at a time so upgrading does not interrupt service.

3. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to remove organization-defined software components after updated versions have been installed.

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Rolling upgrades:
https://www.elastic.co/guide/en/elasticsearch/reference/current/rolling-upgrades.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Installation of patches and updates is performed when there are errors or security vulnerabilities in the current release of the software. When previous versions of software components are not removed from the application server after updates have been installed, an attacker may use the older components to exploit the system.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57563; SV-71839

Comments:

CCI: CCI-002617The organization removes organization-defined software components (e.g. previous versions) after updated versions have been installed.NIST SP 800-53 Revision 4 :: SI-2 (6)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must install security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).
STIG ID: SRG-APP-000456 **Rule ID:** SV-204823r508029_rule **Vul ID:** V-204823
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server checks with a patch management system to install security-relevant software updates within a timeframe directed by an authoritative source.

If the application server does not install security-relevant patches within the time period directed by the authoritative source, this is a finding.

Fix Text:
Steps/Recommendation:

1. For on premises implementation, review all the nodes of the cluster to install security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

2. As part of the hosted Elasticsearch Service offering, Elastic Cloud installs security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

3. If using configuration management tools such as Ansible, Puppet, and Chef among others, the deployment tools must be configured to install security-relevant software updates within the time period directed by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

References:

a. Elasticsearch Service Documentation:
https://www.elastic.co/guide/en/cloud/current/index.html
b. Release notes:
https://www.elastic.co/guide/en/elasticsearch/reference/current/es-release-notes.html
c. STIGs: https://cyber.mil/stigs/

d. NSA Configuration Guides:
https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/
e. CTOs: https://www.cybercom.mil/
f. DTMs: https://www.esd.whs.mil/DD/DoD-Issuances/DTM/

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes) to production systems after thorough testing of the patches within a lab environment. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57561; SV-71837

Comments:

CCI: CCI-002605The organization installs security-relevant software updates within organization-defined time period of the release of the updatesNIST SP 800-53 Revision 4 :: SI-2 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful attempts to modify privileges occur.
STIG ID: SRG-APP-000495 **Rule ID:** SV-204824r508029_rule **Vul ID:** V-204824
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when successful/unsuccessful attempts are made to modify privileges.

If log records are not generated, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Changing privileges of a subject/object may cause a subject/object to gain or lose capabilities. When successful/unsuccessful changes are made, the event needs to be logged. By logging the event, the modification or attempted modification can be investigated to determine if it was performed inadvertently or maliciously.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57439; SV-71711

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful attempts to delete privileges occur.
STIG ID: SRG-APP-000499 **Rule ID:** SV-204825r508029_rule **Vul ID:** V-204825
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when successful and unsuccessful attempts are made to delete privileges.

If log records are not generated, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Deleting privileges of a subject/object may cause a subject/object to gain or lose capabilities. When successful and unsuccessful privilege deletions are made, the events need to be logged. By logging the event, the modification or attempted modification can be investigated to determine if it was performed inadvertently or maliciously.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57441; SV-71713

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when successful/unsuccessful logon attempts occur.
STIG ID: SRG-APP-000503 **Rule ID:** SV-204826r508029_rule **Vul ID:** V-204826
Severity: CAT II

Documentable: No

Check Content:
Review product documentation and the system configuration to determine if the application server generates log records on successful and unsuccessful logon attempts by users.

If logon attempts do not generate log records, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:

Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Logging the access to the application server allows the system administrators to monitor user accounts. By logging successful/unsuccessful logons, the system administrator can determine if an account is compromised (e.g., frequent logons) or is in the process of being compromised (e.g., frequent failed logons) and can take actions to thwart the attack.

Logging successful logons can also be used to determine accounts that are no longer in use.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57443; SV-71715

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records for privileged activities.
STIG ID: SRG-APP-000504 **Rule ID:** SV-204827r508029_rule **Vul ID:** V-204827
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records for privileged activities.

If log records are not generated for privileged activities, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as

xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Privileged activities would occur through the management interface. This interface can be

web-based or can be command line utilities. Whichever method is utilized by the application server, these activities must be logged.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57445; SV-71717

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application must generate log records showing starting and ending times for user access to the application server management interface.
STIG ID: SRG-APP-000505 **Rule ID:** SV-204828r508029_rule **Vul ID:** V-204828
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records showing starting and ending times for user access to the management interface.

If log records are not generated showing starting and ending times of user access to the management interface, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For

dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Determining when a user has accessed the management interface is important to determine the timeline of events when a security incident occurs. Generating these events, especially if the management interface is accessed via a stateless protocol like HTTP, the log events will be generated when the user performs a logon (start) and when the user performs a logoff (end). Without these events, the user and later investigators cannot determine the sequence of events and therefore cannot determine what may have happened and by whom it

may have been done.

The generation of start and end times within log events allow the user to perform their due diligence in the event of a security breach.

Legacy Ids: V-57481; SV-71757

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records when concurrent logons from different workstations occur to the application server management interface.
STIG ID: SRG-APP-000506 **Rule ID:** SV-204829r508029_rule **Vul ID:** V-204829
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records showing concurrent logons from different workstations to the management interface.

If concurrent logons from different workstations are not logged, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be

explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Being able to work on a system through multiple views into the application allows a user to work more efficiently and more accurately. Before environments with windowing capabilities or multiple desktops, a user would log onto the application from different workstations or terminals. With today's workstations, this is no longer necessary and may signal a compromised session or user account.

When concurrent logons are made from different workstations to the management interface, a log record needs to be generated. This allows the system administrator to investigate the incident and to be aware of the incident.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57483; SV-71759

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must generate log records for all account creations, modifications, disabling, and termination events.
STIG ID: SRG-APP-000509 **Rule ID:** SV-204830r508029_rule **Vul ID:** V-204830
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and the system configuration to determine if the application server generates log records when accounts are created, modified, disabled, or terminated.

If the application server does not generate log records for account creation, modification, disabling, and termination, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable audit logging:
Set xpack.security.audit.enabled to true in elasticsearch.yml.
Restart Elasticsearch.

Note: Audit logs are disabled by default. One must explicitly enable audit logging. If configured, auditing settings must be set on every node in the cluster. Static settings, such as xpack.security.audit.enabled, must be configured in elasticsearch.yml on each node. For dynamic auditing settings, use the cluster update settings API to ensure the setting is the same on all nodes.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. To enable Kibana audit logging:
Set xpack.security.audit.enabled to true in kibana.yml.

3. If using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm, configure the application server to generate log records for all account creations, modifications, disabling, and termination events.

References:

a. Enabling audit logging:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/enable-audit-logging.html
b. Kibana Audit Logs:
https://www.elastic.co/guide/en/kibana/current/xpack-security-audit-logging.html
c. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
d. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html
e. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
f. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The maintenance of user accounts is a key activity within the system to determine access and privileges. Through changes to accounts, an attacker can create an account for persistent access, modify an account to elevate privileges or terminate/disable an account(s) to cause a DoS for user(s). To be able to track and investigate these actions, log records must be generated for any account modification functions.

Application servers either provide a local user store, or they can integrate with enterprise user stores like LDAP. As such, the application server must be able to generate log records on account creation, modification, disabling, and termination.

Legacy Ids: V-57485; SV-71761

Comments:

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: Application servers must use NIST-approved or NSA-approved key management technology and processes.
STIG ID: SRG-APP-000514 **Rule ID:** SV-204831r508029_rule **Vul ID:** V-204831
Severity: CAT II

Documentable: No

Check Content:
Review application server configuration and the NIST FIPS certificate to validate the application server uses NIST-approved or NSA-approved key management technology and processes when producing, controlling or distributing symmetric and asymmetric keys.

If the application server does not use this NIST-approved or NSA-approved key management technology and processes, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: An asymmetric encryption key must be protected during transmission. The public portion of an asymmetric key pair can be freely distributed without fear of compromise, and the private portion of the key must be protected. The application server will provide software libraries that applications can programmatically utilize to encrypt and decrypt information. These application server libraries must use NIST-approved or NSA-approved key management technology and processes when producing, controlling, or distributing symmetric and asymmetric keys.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57543; SV-71819

Comments:

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations and standards.NIST SP 800-53 Revision 4 :: SC-13

Rule Title: The application server must use DoD- or CNSS-approved PKI Class 3 or Class 4 certificates.
STIG ID: SRG-APP-000514 **Rule ID:** SV-204832r508029_rule **Vul ID:** V-204832
Severity: CAT II

Documentable: No

Check Content:
Review the application server configuration to determine if the application server utilizes approved PKI Class 3 or Class 4 certificates.

If the application server is not configured to use approved DoD or CNS certificates, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Use a DoD PKI Class 3 or Class 4 certificate in both Elasticsearch and Kibana.

3. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

4. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

5. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

6. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.

- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Class 3 PKI certificates are used for servers and software signing rather than for identifying individuals. Class 4 certificates are used for business-to-business transactions. Utilizing unapproved certificates not issued or approved by DoD or CNS creates an integrity risk. The application server must utilize approved DoD or CNS Class 3 or Class 4 certificates for software signing and business-to-business transactions.

Legacy Ids: V-57545; SV-71821

Comments:

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.NIST SP 800-53 Revision 4 :: SC-13

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must, at a minimum, transfer the logs of interconnected systems in real time, and transfer the logs of standalone systems weekly.
STIG ID: SRG-APP-000515 **Rule ID:** SV-204833r508029_rule **Vul ID:** V-204833
Severity: CAT II

Documentable: No

Check Content:
Verify the log records are being off-loaded, at a minimum of real time for interconnected systems and weekly for standalone systems.

If the application server is not meeting these requirements, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch can be configured to provide redundancy by storing the Elasticsearch data on different media to support off-load interconnected systems in real time and off-load

standalone systems weekly, at a minimum. Verify that standalone system logs are received when those systems are re-connected and automatically resumed when connectivity is restored after a loss in connectivity.

Reference:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/current/resiliency.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration. Protecting log data is important during a forensic investigation to ensure investigators can track and understand what may have occurred. Off-loading should be set up as a scheduled task but can be configured to be run manually, if other processes during the off-loading are manual.

Off-loading is a common process in information systems with limited log storage capacity.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57425; SV-71697

Comments:

CCI: CCI-001851The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.NIST SP 800-53 Revision 4 :: AU-4 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must be configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.
STIG ID: SRG-APP-000516 **Rule ID:** SV-204834r508029_rule **Vul ID:** V-204834
Severity: CAT II

Documentable: No

Check Content:
Review the application server documentation and configuration to determine if the application server is configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.

If the application server is not configured in accordance with security configuration settings, this is a finding.

Fix Text:
Step/Recommendation:

1. It is up to the organization to ensure the application server is configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including Security Technical Implementation (STIGs), NSA configuration guides, CYBERCOM Task Order (CTOs), and Directive-Type Memorandum (DTM).

References:

a. STIGs: https://cyber.mil/stigs/
b. NSA Configuration Guides:
https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/
c. CTOs: https://www.cybercom.mil/
d. DTMs: https://www.esd.whs.mil/DD/DoD-Issuances/DTM/

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Configuring the application to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the application, including the parameters required to satisfy other security control requirements.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups, certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57499; SV-71775

Comments:

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Application Server Security Requirement Guide:: Version 3, Revision 1 Benchmark Date: 10 December 2021 :: Version 1,
Rule Title: The application server must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
STIG ID: SRG-APP-000416 **Rule ID:** SV-220326r508029_rule **Vul ID:** V-220326
Severity: CAT II

Documentable: No

Check Content:
Review application server documentation to verify that the application server is using NSA-approved cryptography to protect classified data and applications resident on the device.

If the application server is not using NSA-approved cryptography for classified data and applications, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see

The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Cryptography is only as strong as the encryption modules/algorithms employed to encrypt the data. Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data.

NSA has developed Type 1 algorithms for protecting classified information. The Committee on National Security Systems (CNSS) National Information Assurance Glossary (CNSS Instruction No. 4009) defines Type 1 products as:

"Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA-approved algorithms
are used to protect systems requiring the most stringent protection mechanisms."

NSA-approved cryptography is required to be used for classified information system processing.

The application server must utilize NSA-approved encryption modules when protecting classified data. This means using AES and other approved encryption modules.

Organization is responsible for satisfying all the security controls for the external dependencies, like but not limited to, identity provider, operating system, backups,

certificates, etc. For dependencies, the control implementation can either be fully inherited or a hybrid with another control provider.

Legacy Ids: V-57541; SV-71817

Comments:

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations and standards.NIST SP 800-53 Revision 4 :: SC-13