John Darragh <darragh@entrotech.net>

Re: Potential Sensitive Information Disclosure

Lon Soh <lon.soh@lacity.org> Mon, Jul 10, 2023 at 10:37 AM
To: ITA Information Security Office <ita.security@lacity.org>, John Darragh <darragh@entrotech.net>, Alexander Wikstrom <alexander.wikstrom@lacity.org>

I believe John Darragh, our developer/contractor, has previously updated you on this issue. At any rate, I'm looping in John again. Perhaps he can resend the update, or perform any further steps to mitigate issue?

****

Lon L. Soh

Senior Systems Analyst II

Information Technology Division

Los Angeles Department of Transportation
213.972-8454

On Mon, Jul 10, 2023 at 10:25 AM ITA Information Security Office <ita.security@lacity.org> wrote:

> Hello Lon,
> Please provide an update on this alert.
>
> Thank you,
>
> Information Security Office
> Information Technology Agency
> City of Los Angeles
> ita.security@lacity.org
>
> On Wed, May 17, 2023 at 9:29 AM ITA Information Security Office <ita.security@lacity.org> wrote:
>
> > Hello DOT cybersecurity coordinator(s),
> >
> > A trusted third party vendor has recently identified the site tdm.ladot.lacity.org as being vulnerable to IDOR attacks that lead to information disclosure.
> >
> > Please investigate and remediate as soon as possible. Recommendations and reference guides have been provided below.
> >
> > ==========

Severity: Medium

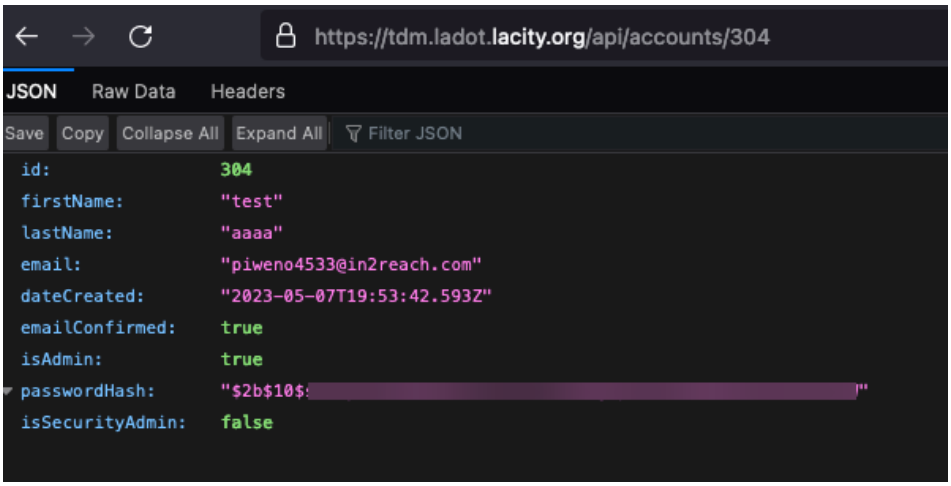
Analysis:

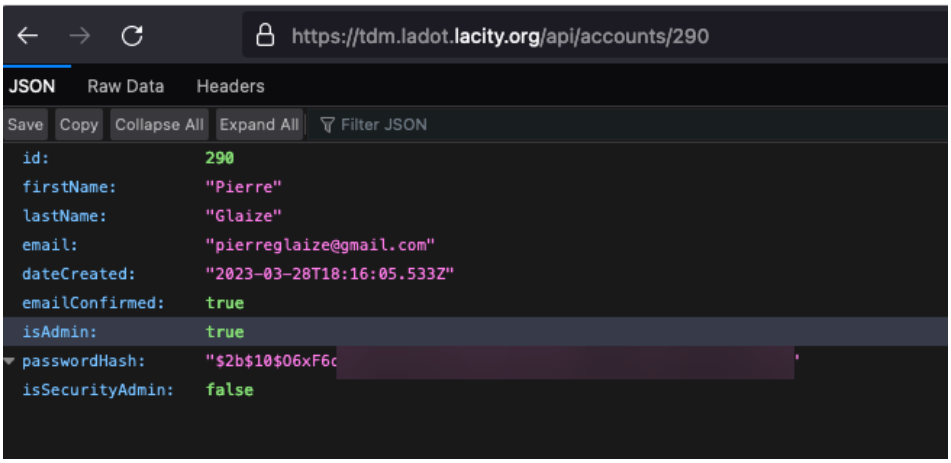
The endpoint at https://tdm.ladot.lacity.org/api/accounts/ suffers from a possible IDOR vulnerability that allows information disclosure.

An IDOR (Insecure Direct Object Reference) attack is a type of vulnerability found in web applications. It occurs when an application exposes a direct reference to an internal object, such as a database record or file, without proper authorization checks. By manipulating the object references in requests, an attacker can access resources they are not authorized to access.

Steps to Reproduce

1. Login to https://tdm.ladot.lacity.org/
2. Navigate to https://tdm.ladot.lacity.org/api/accounts/304 or https://tdm.ladot.lacity.org/api/accounts/290 observe the information of other users disclosed





The Open Web Application Security Project (OWASP) provides excellent guidance on safeguarding against many web app security vulnerabilities including IDOR, XSS, and SQL injection among others. Please see the guides below for more information and remediation guidance.

Recommendations:

- Investigate the reported vulnerability and review the links in the references.
- Consider the following to safeguard against IDOR attacks:

- Implement Proper Access Controls: Use a robust access control mechanism to ensure that users can only access resources or data that they are authorized to view or modify. Avoid relying solely on client-side checks and enforce server-side validation.
- Validate User Input: Validate and sanitize user input to prevent malicious actors from manipulating parameters or changing object references in requests. Implement input validation at both the client and server sides.
- Use Indirect Object References: Avoid using direct object references, such as database IDs or file names, in URLs or other user-accessible parameters. Instead, use indirect references or tokens that are securely mapped to the actual resources on the server.
- Employ Role-Based Access Control (RBAC): Implement RBAC to define and enforce granular access permissions based on user roles. This ensures that each user can only access the resources or functionality necessary for their role.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html#proposition

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References

Please disregard the following:
#1981103

Thank you,

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