usd-2021-0015

Advisory ID: usd-2021-0015
CVE Number: CVE-2021-33617
Affected Product: Password Manager
Affected Version: < Version 11.2 Build
Vulnerability Type: User Enumeration
Security Risk: Low
Vendor URL: https://www.manageengine.com/products/passwordmanagerpro/
Vendor Status: Fixed

Description

The ManageEngine Password Manager Pro web application allows the determination of valid logon names. This can be achieved by passing either an existing or non-existing user name to the application and view its corresponding response.

User Enumeration vulnerabilities occur if observable discrepancies of an application's behavior allow to determine whether an user account is existent within an application. Such vulnerabilities can be often exploited to generate a list of valid logon names, potentially acting as foothold for further attacks.

The *Password Manager Pro* exposes an endpoint that enables an unauthenticated malicious actor to determine whether an *userName* is existent within the application.

Proof of Concept (PoC)

The *Password Manager Pro* exposes an endpoint that responds with different contents if a *userName* parameter at https://example.com/login/AjaxResponse.jsp?RequestType=GetUserDomainName&userName=[VALUE] holds an existing user name or not.

1. Non-existent user: https://example.com/login/AjaxResponse.jsp?RequestType=GetUserDomainName&userName=non.existent

2.Existing user: https://example.com/login/AjaxResponse.jsp?RequestType=GetUserDomainName&userName=max.mustermann

Fix

It is recommended to use generic error messages that do not allow to draw conclusions about logon names.

References

- https://cwe.mitre.org/data/definitions/203.html
- https://www.gnucitizen.org/blog/username-enumeration-vulnerabilities/

Timeline

- 2021-04-01: This vulnerability was identified by Marcus Nilsson.
- 2021-04-15: Advisory submitted to vendor via e-mail.
- 2021-05-28: CVE-2021-33617 is assigned
- 2021-07-07: Security fix is released with Version 11.2 Build 11200: *„A user enumeration issue has been fixed".*
- 2021-07-30: Security advisory released by usd AG.

Credits

This security vulnerability was found by Marcus Nilsson of usd AG.

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this security advisory is provided „as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.