ManageEngine Key Manager Plus Cross-Site Scripting Vulnerability (CVE-2021-28382)

Exploits
Jun 11 | Written By Matt Mathur

This is a summary of the second stored cross-site scripting vulnerability I discovered while testing several Zoho-owned ManageEngine products. This vulnerability exists in the Key Manager Plus Version 6000.

Summary

Recently I discovered a stored Cross-Site Scripting vulnerability in the Zoho-owned ManageEngine Key Manager Plus for Version 6000 (CVE-2021-28382). The vulnerability exists in any of a user's details fields when they are imported from Active Directory. This can be performed in one of the name fields or the email field, and is executed when visiting the /apiclient/index.jsp#/Settings/UserManagement page. After this page loads, the user's details are loaded with unescaped content, allowing for malicious JavaScript to be reflected back to users.

Proof of Concept

The vulnerability can be triggered by inserting html content, specifically script tags, into the first name, last name, or email field of an Active Directory user. The following was inserted as a proof of concept to reflect the user's cookie in an alert box:

<script>alert(document.cookie)</script>

An example of this in the Last Name field of one such user can be seen in Figure 1:

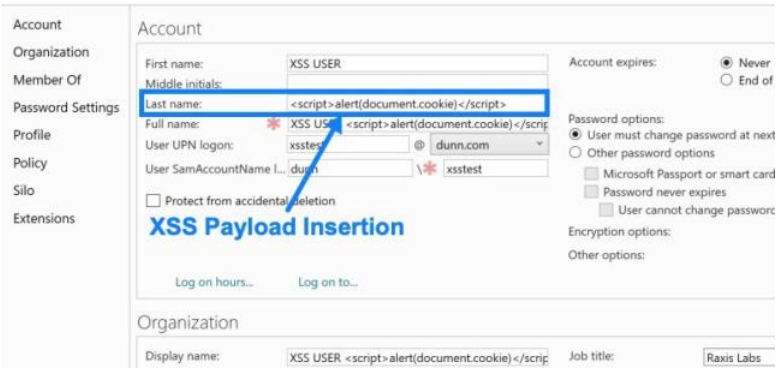

Figure 1: Stored XSS Payload

After that user's details load on the UserManagement page, the HTML is then presented unescaped on the web page, which allows the script tags to be loaded as valid JavaScript. The unescaped HTML, as loaded, can be seen in Figure 2:

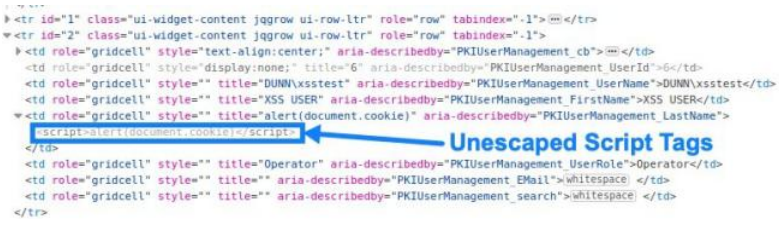

Figure 2: Unescaped JavaScript Tags

After loading the UserManagement page, the malicious content is executed, as shown in Figure 3:

Raxis discovered this vulnerability on Manage Engine Key Manager Plus 6000 (6.0.0), but any version below 6001 could be vulnerable when importing users from Active Directory.

Remediation

Upgrade ManageEngine Key Manager Plus to version 6001 or later immediately. Version 6001 can be found here: https://www.manageengine.com/key-manager/release-notes.html#6001

Disclosure Timeline

- **March 5, 2021** – Vulnerability reported to Zoho
- **March 8, 2021** – Zoho begins investigation into report
- **March 13, 2021** – Zoho releases version 6001 to mitigate vulnerability
- **March 15, 2021** - CVE-2021-28382 assigned to this vulnerability

CVE Links

- **Mitre CVE** - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28382
- **NVD** - https://nvd.nist.gov/vuln/detail/CVE-2021-28382

If you found this post interesting, you might like these as well:

- Cross-Site Scripting Vulnerability in ManageEngine AD Self Service Plus (CVE-2021-27956)
- SonicWall Patches Three Zero-Day Vulnerabilities
- New Metasploit Module: Microsoft Remote Desktop Web Access Authentication Timing Attack

CVE-2021-28382 | vulnerability management | ManageEngine | Zoho | Matt Dunn | cross-site scripting

Matt Mathur

What You Need to Know (But Were Afraid to Ask) about Raxis Web App Testing

Raxis' Transporter Enables Remote Penetration Testing

Careers
Raxis News and Coverage
Raxis FAQ

Glossary
Boscloner
Meet the Raxis Team

LET'S TALK