ManageEngine Applications Manager Stored Cross-Site Scripting Vulnerability (CVE-2021-31813)

Security Recommendations
Jun 25 | Written By Matt Mathur

This is a summary of the third stored cross-site scripting vulnerability I discovered while testing several Zoho-owned ManageEngine products. This vulnerability exists in the Applications Manager product.

Summary

Recently I discovered a stored Cross-Site Scripting vulnerability in ManageEngine Applications Manager. The vulnerability exists in a users' name fields when they are imported from Active Directory. This can be performed in any of the name fields and is executed when selecting the user for import on /admin/userconfiguration.do after fetching users from the domain. After the import loads and the user is selected, the user's name is loaded with unescaped content, allowing malicious JavaScript to be reflected back to the user.

Proof of Concept

The vulnerability can be triggered by inserting html content, specifically script tags, into the first or last name 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:

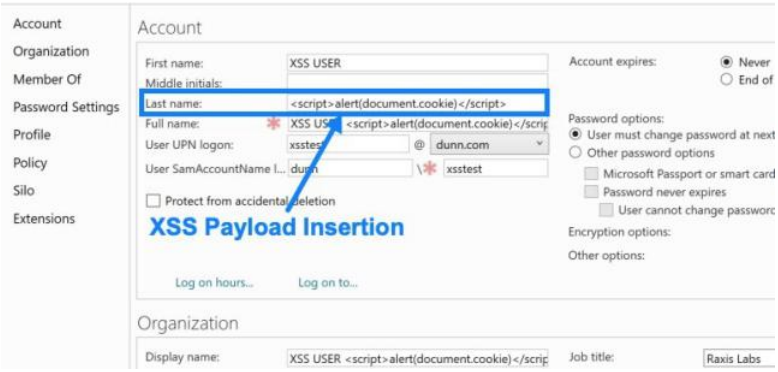

Figure 1: Stored XSS Payload

After that user is selected and the details load on the "User Imported from Active Directory" page, the HTML is 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 selected user, the malicious content is executed, as shown in Figure 3:

Raxis discovered this vulnerability on Manage Engine Applications Manager 15, Build 15080.

Remediation

Upgrade ManageEngine Applications Manager to Version 15.1 Build 15130 or later immediately which can be found here:

- Download Link: https://www.manageengine.com/products/applications_manager/download.html
- Release Notes: https://www.manageengine.com/products/applications_manager/release-notes.html

Disclosure Timeline

- **March 18, 2021** – Vulnerability reported to Zoho
- **March 18, 2021** – Zoho begins investigation into report
- **April 27, 2021** – Zoho releases fixed version 15.1 Build 15130
- **April 27, 2021**- CVE-2021-31813 is assigned to this vulnerability

CVE Links

- **Mitre CVE** - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31813
- **NVD** - https://nvd.nist.gov/vuln/detail/CVE-2021-31813

Be sure to check out these related articles:

- ManageEngine Key Manager Plus Cross-Site Scripting Vulnerability (CVE-2021-28382)
- Cross-Site Scripting Vulnerability in ManageEngine AD Self Service Plus (CVE-2021-27956)
- New Metasploit Module: Microsoft Remote Desktop Web Access Authentication Timing Attack

CVE-2021-31813 | vulnerability management | ethical hacking

Matt Mathur

〈 What Companies Should be Telling Investors about Cybersecurity

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

Terms and Policies