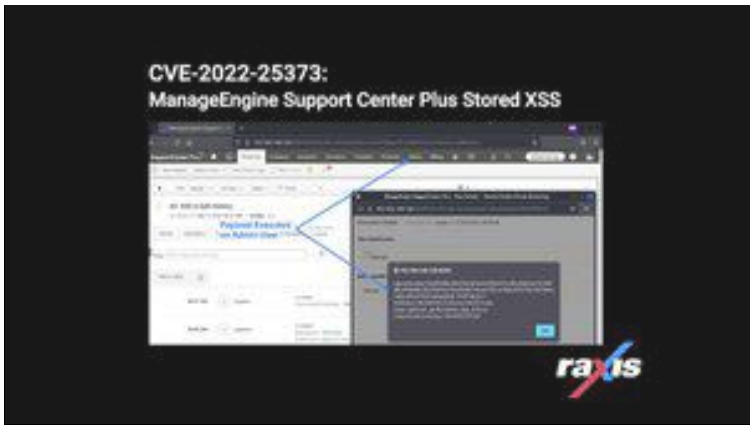
CVE-2022-25373: ManageEngine Support Center Plus Stored Cross-Site Scripting (XSS)

Exploits
Jul 6 | Written By Matt Mathur



I'm Matt Dunn, lead penetration tester at Raxis. Recently, I discovered a stored XSS in Support Center Plus. Here's how a malicious actor might exploit it — and what you can do to prevent it.

Summary

A low-privileged user (e.g., the default guest user) can inject arbitrary JavaScript into the description of a new Request. When another user (including a high privileged user) views that request's edit history, the

The vulnerability can be triggered by inserting html content in the description field of a new request. The payload I inserted as a guest user was:

">

This payload being inserted is shown in Figure 1:

Figure 1: Payload Inserted as Guest User

When another user (in this case an admin) views that request's edit history, the JavaScript is executed in the context of the new user's browser, as shown in Figure 2:

Figure 2: Payload Execution in Admin User Session

This vulnerability allows any low privileged user to execute JavaScript on higher privileged or other low privilege user's browsers once they view a request's edit history. While the payload used here launches an alert box with the page's cookie values, more dangerous payloads could be executed in this context as well.

Affected Versions

Raxis discovered this vulnerability on Manage Engine Support Center 11.0 Build 11019.

Remediation

Upgrade ManageEngine AD Support Center Plus to Version 11.0 Build 11020 or later immediately which can be found here:

- Download Link: https://www.manageengine.com/products/support-center/service-packs.html
- Release Notes: https://pitstop.manageengine.com/portal/en/community/topic/manageengine-supportcenter-plus-version-11-0-build-11020-released

Disclosure Timeline

- February 2, 2022 – Vulnerability reported to Zoho
- February 14, 2022 – Zoho begins investigation into report
- February 21, 2022- CVE-2022-25373 is assigned to this vulnerability
- March 22, 2022 – Zoho releases fixed version 11.0 Build 11020

CVE Links

- Mitre CVE - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25373
- NVD - https://nvd.nist.gov/vuln/detail/CVE-2022-25373

- Exploiting Dirty Pipe (CVE-2022-0847)
- Why We Take Simultaneous Sessions Seriously

CVE-2022-25373 | Matt Dunn | cross-site scripting | ManageEngine

Matt Mathur

‹ CVE-2022-26653 & CVE-2022-26777: ManageEngine Remote Access Plus Guest User Insecure Direct Object References

Raxis Earns Five-Star Rating ›