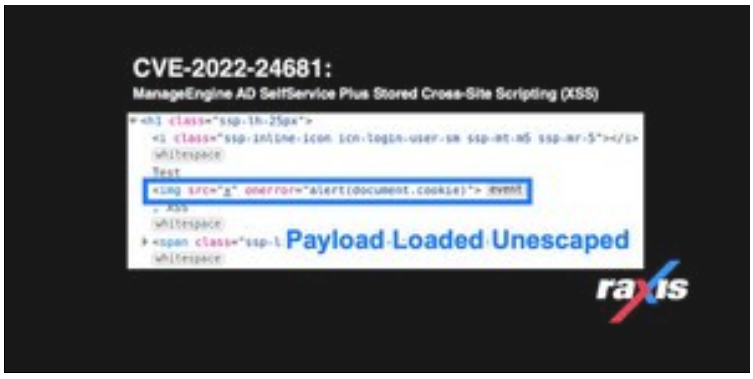
CVE-2022-24681: ManageEngine AD SelfService Plus Stored Cross-Site Scripting (XSS)

Exploits
May 17 | Written By Matt Mathur



I'm Matt Dunn, a lead penetration tester here at Raxis. Recently, I discovered a stored Cross-Site Scripting vulnerability in Zoho's ManageEngine AD SelfService Plus.

Summary

The vulnerability exists in the /accounts/authVerify page, which is used for the forgot password, change password, and unlock account functionalities.

reflect the user's cookie in an alert box:

****

An example of this in the Last Name field of one such user is shown in Figure 1:

Figure 1: Stored XSS Payload

Figure 2: Unescaped JavaScript Tags

After the user attempts to reset their password, the malicious content is executed, as shown in Figure 3:

Figure 3: JavaScript Execution to Display User's Cookie in an Alert Box

If the user must change their password on login, the malicious content is executed, as shown in Figure 4:

Figure 4: Payload Execution on Change Password Page

If the user attempts to unlock their account, the malicious content is executed, as shown in Figure 5:

Figure 5: Payload Execution on Account Unlock

Affected Versions

Upgrade ManageEngine AD SelfService Plus to Version 6.1 Build 6121 or later immediately:

- Download Link: https://www.manageengine.com/products/self-service-password/download.html
- Release Notes: https://www.manageengine.com/products/self-service-password/release-notes.html#6121

Disclosure Timeline

- January 22, 2022 – Vulnerability reported to Zoho
- January 22, 2022 – Zoho begins investigation into report
- February 9, 2022- CVE-2022-24681 is assigned to this vulnerability
- March 7, 2022 – Zoho releases fixed version 6.1 Build 6121

CVE Links

- Mitre CVE - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24681
- NVD - https://nvd.nist.gov/vuln/detail/CVE-2022-24681

If you found this article interesting, read more by and about Matt Dunn:

- Why We Take Simultaneous Sessions Seriously
- Reporting Tools for Large Penetration Tests
- New Metasploit Module: Azure AD Login Scanner
- Meet the Team: Matt Dunn, Lead Penetration Tester

cross-site scripting | ManageEngine | vulnerability management

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

Careers
Raxis News and Coverage
Raxis FAQ

Glossary
Boscloner
Meet the Raxis Team

LET'S TALK

Terms and Policies