Cross-Site Scripting Vulnerability in ManageEngine AD Self Service Plus (CVE-2021-27956)

Exploits
May 20 | Written By Matt Mathur

This is a summary of the first stored cross-site scripting vulnerability I discovered while testing several Zoho-owned ManageEngine products. This vulnerability exists in the AD Self Service Plus Version 6.1.

Summary

Recently I discovered a stored cross-site scripting (XSS) vulnerability in the Zoho-owned ManageEngine AD Self Service Plus for Version 6.1 (CVE-2021-27956). The vulnerability exists in the email field of search results on the page: /webclient/index.html#/directory-search. After searching for a user, if the "More" tab is clicked, the email field is 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, in this case script tags, into the 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 on one such user is shown in Figure 1:

Figure 1: Stored XSS Payload

After searching for that user, 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 is shown in Figure 2:

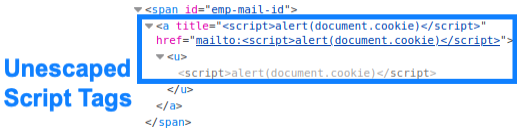
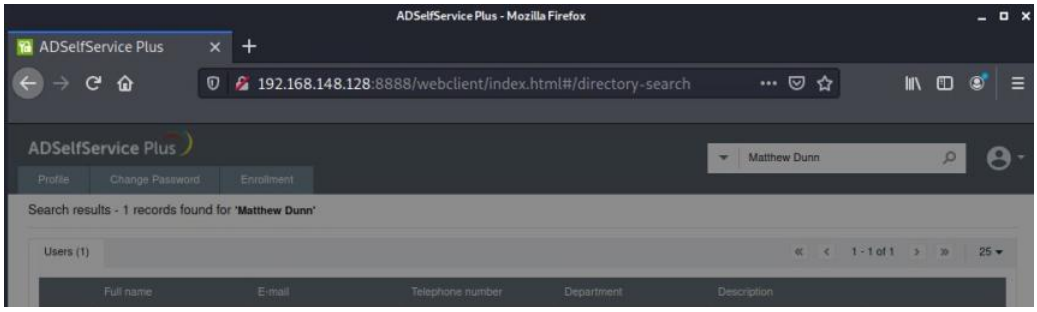
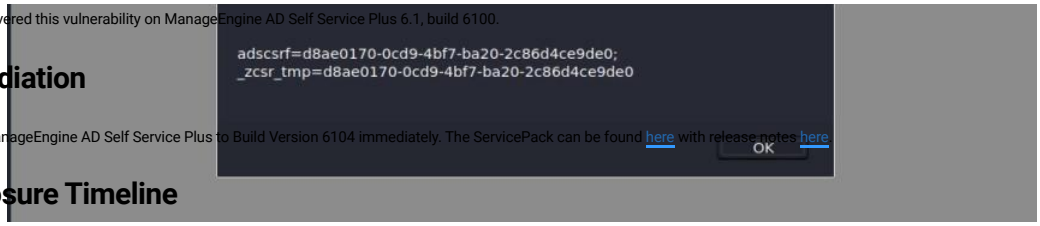


Figure 2: Unescaped JavaScript Tags

After loading the search page, clicking the "More" tab triggers the vulnerability, which is shown in Figure 3:



Raxis discovered this vulnerability on ManageEngine AD Self Service Plus 6.1, build 6100.



Remediation

Upgrade ManageEngine AD Self Service Plus to Build Version 6104 immediately. The ServicePack can be found here with release notes here.

Disclosure Timeline

- **February 19, 2021 –** Vulnerability reported to Zoho
- **February 19, 2021 –** Zoho begins investigation into report
- **March 5, 2021 -** CVE-2021-27956 assigned to this vulnerability
- **May 8, 2021 –** Zoho releases patch for this vulnerability

CVE Links

- **Mitre CVE -** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27956
- **NVD -** https://nvd.nist.gov/vuln/detail/CVE-2021-27956

Did you find this post helpful? If so, you may also be interested in:

- SonicWall Patches Three Zero-Day Vulnerabilities
- NSA, FBI, CISA Statement on Russian SVR Activity
- New Metasploit Module: Microsoft Remote Desktop Web Access Authentication Timing Attack

CVE-2021-27956 | Matt Dunn | vulnerability management | cross-site scripting | cybersecurity tips | Zoho | ManageEngine

Matt Mathur

Glossary
Boscloner
Meet the Raxis Team

LET'S TALK

Terms and Policies