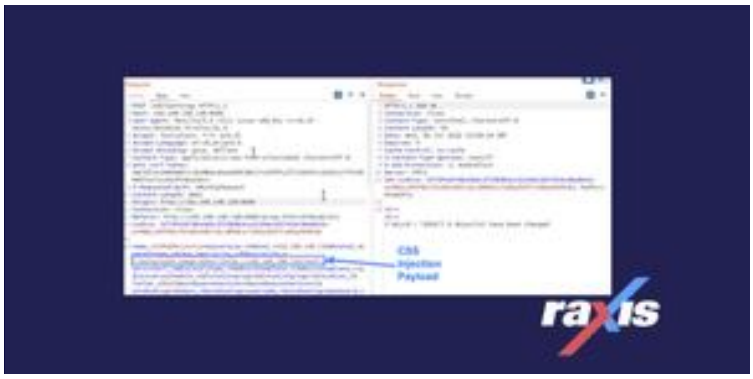
CVE-2022-35739: PRTG Network Monitor Cascading Style Sheets (CSS) Injection

Exploits
Oct 21 | Written By Matt Mathur



I'm Matt Mathur, lead penetration tester here at Raxis. I recently discovered a cascading style sheet (CSS) injection vulnerability in PRTG Network Monitor.

Summary

PRTG Network Monitor does not prevent custom input for a device's icon, which can be modified to insert arbitrary content into the style tag for that device. When the device page loads, the arbitrary CSS is inserted into the style tag, loading malicious content. Due to PRTG Network Monitor preventing " characters, and from modern browsers disabling JavaScript support in style tags, this vulnerability could not be escalated into a Cross-Site Scripting vulnerability.

Proof of Concept

Figure 1: CSS Injection Payload

When the device's icon is then loaded in any subsequent pages (e.g., the Devices page), the content is loaded unescaped inside of the style tag, as shown in Figure 2:

Figure 2: Payload Insertion Point

Figure 3: Payload Execution Causing HTTP Request to Controlled Server

The impact of this vulnerability is less severe due to modern browsers preventing JavaScript in style tags, and from PRTG Network Monitor preventing " characters in the payload. These steps prevent this vulnerability from being escalated into a Cross-Site Scripting vulnerability.

Affected Versions

Raxis discovered this vulnerability on PRTG Network Monitor version 22.2.77.2204.

Remediation

A fix for CVE-2022-35739 has not been released. When a fix is released, upgrade to the newest version to fully remediate the vulnerability. In the meantime, Raxis recommends keeping a small list of users who can edit devices to limit the impact of the vulnerability. CVE-2022-35739 has minimal damage potential and is difficult to execute, and thus does not warrant additional protections while waiting for a remediation.

Disclosure Timeline

- **July 7, 2022** – Vulnerability reported to Paessler Technologies.
- **July 8, 2022** – Paessler Technologies begins investigating vulnerability.
- **July 14, 2022** - CVE-2022-35739 assigned to this vulnerability.
- **August 8, 2022** – Outreach to Paessler Technologies without response.
- **October 4, 2022** – Second outreach to Paessler Technologies without response.
- **October 7, 2022** – Third outreach to Paessler Technologies without response.

- **Mitre CVE** - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35739
- **NVD**: https://nvd.nist.gov/vuln/detail/CVE-2022-35739

If you found this article useful, check out these others by Matt Mathur:

- CVE-2022-26653 & CVE-2022-26777: ManageEngine Remote Access Plus Guest User Insecure Direct Object References
- CVE-2022-25373: ManageEngine Support Center Plus Stored Cross-Site Scripting (XSS)
- CVE-2022-25245: ManageEngine Asset Explorer Information Leakage

CVE 2022-35739 | vulnerability management | Matt Mathur | exploit

Matt Mathur

‹ RAXIS THREAT ALERT: VULNERABILITY IN OPENSSL v3.0.x

What to Expect with a Raxis Wireless Penetration Test ›

Careers
Raxis News and Coverage
Raxis FAQ

Glossary

Terms and Policies