Security Advisory 2022-077

Several High Vulnerabilities in Splunk Enterprise

November 04, 2022 — v1.0

TLP:CLEAR

History:

- *04/11/2022 — v1.0 – Initial publication*

Summary

On November 2, 2022, Splunk released the quarterly Security Patch Update which included nine HIGH severity vulnerabilities. The most severe vulnerabilities, which have a CVSS score of `8.8` out of 10, are `CVE-2022-43571` for Remote Code Execution (RCE) through dashboard PDF generation component, `CVE-2022-43570` for XML External Entity Injection through a custom View and `CVE-2022-43568` for Reflected Cross-Site Scripting via the radio template.

Technical Details

`CVE-2022-43571` allows an authenticated user to execute arbitrary code through the dashboard PDF generation component.

`CVE-2022-43570` allows an authenticated user to perform an extensible markup language (XML) external entity (XXE) injection via a custom View. The XXE injection causes Splunk Web to embed incorrect documents into an error.

`CVE-2022-43568` a View allows for a Reflected Cross Site Scripting via JavaScript Object Notation (JSON) in a query parameter when `output_mode=radio` .

Mitigation and Workarounds

`CVE-2022-43571` - No mitigation or workarounds available.

`CVE-2022-43570` - Workarounds include restricting who can upload lookup files and disabling Splunk Web. The vulnerability affects instances with Splunk Web enabled. [2,3]

`CVE-2022-43568` - The vulnerability affects instances with Splunk Web enabled, disabling Splunk Web is a possible workaround. [2,3]

Recommendations

CERT-EU strongly recommends upgrading Splunk Enterprise to the version 8.1.12, 8.2.9, 9.0.2 or higher.

References

[1] https://www.splunk.com/en_us/product-security.html

[2] https://docs.splunk.com/Documentation/Splunk/latest/Security/DisableunnecessarySplunkcomponents

[3] https://docs.splunk.com/Documentation/Splunk/latest/Admin/Webconf