Remote code execution (RCE) in Splunk Enterprise through Insecure XML Parsing

Advisory ID: SVD-2023-1104

CVE ID: CVE-2023-46214

Published: 2023-11-16

Last Update: 2023-12-12

CVSSv3.1 Score: 8.0, High

CVSSv3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

CWE: CWE-91

Bug ID: SPL-241695

Description

In Splunk Enterprise versions below 9.0.7 and 9.1.2, Splunk Enterprise does not safely sanitize extensible stylesheet language transformations (XSLT) that users supply. This means that an attacker can upload malicious XSLT which can result in remote code execution on the Splunk Enterprise instance.

Solution

Upgrade Splunk Enterprise to either 9.0.7 or 9.1.2.

Splunk is actively monitoring and patching Splunk Cloud Platform instances.

Product Status

Product	Version	Component	Affected Version	Fix Version
Splunk Enterprise	9.0	Splunk Web	9.0.0 to 9.0.6	9.0.7
Splunk Enterprise	9.1	Splunk Web	9.1.0 to 9.1.1	9.1.2
Splunk Cloud	-	Splunk Web	Versions below 9.1.2308	9.1.2308

Mitigations and Workarounds

If you cannot upgrade, limit the ability of search job requests to accept XML stylesheet language (XSL) as valid input.

Edit the `web.conf` configuration file and add the following configuration on instances where you want to limit the ability of search job requests to accept XSL:

```
[settings]
enableSearchJobXslt = false
```

For more information on modifying the web.conf configuration file, see How to edit a configuration file and the web.conf configuration specification. For earlier Splunk Enterprise versions, review the web.conf specification for availability of the `enableSearchJobXslt` setting.

Detections

- Splunk App for Lookup File Editing RCE via User XSLT
- Splunk RCE via User XSLT

Severity

Splunk rates this vulnerability a 8.0, High, with a CVSSv3.1 vector of CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H.

Acknowledgments

Alex Hordijk

Changelog

- 2023-12-12: Added credit
- 2023-11-22: Added Splunk RCE via User XSLT detection
- 2023-11-21: Updated Mitigations
- 2023-11-20: Added relevant detection link

Email **RSS Feed** **Support**

Legal Privacy Website Terms of Use