Security Advisory 2025-013

Remote Code Execution Vulnerability in Splunk

2025-03-27 — v1.0

TLP:CLEAR

History:

- *27/03/2025 — v1.0 – Initial publication*

Summary

On March 26, 2025, Splunk released a security advisory addressing a vulnerability in Splunk Enterprise and Splunk Cloud Platform that allows low-privileged users to perform Remote Code Execution (RCE) [1,2].

It is recommended updating as soon as possible.

Technical Details

The vulnerability `CVE-2025-20229`, with a CVSS Score of 8.0, stems from missing authorisation checks in the file upload process to the `$SPLUNK_HOME/var/run/splunk/apptemp` directory. It allows low-privileged users to execute arbitrary code remotely by uploading malicious files to this specific directory on the server.

Products Affected

The following products and versions are affected:

- Splunk Enterprise from 9.1.0 to 9.1.7, from 9.2.0 to 9.2.4, and from 9.3.0 to 9.3.2
- Splunk Cloud Platform from 9.1.2312 to 9.1.2312.207, from 9.2.2403 to 9.2.2403.113, from 9.2.2406 to 9.2.2406.107 and from 9.3.2408 to 9.3.2408.103

Recommendations

CERT-EU recommends upgrading affected server to the latest version as soon as possible.

References

[1] https://advisory.splunk.com/advisories/SVD-2025-0301

[2] https://www.cve.org/CVERecord?id=CVE-2025-20229