VULNERABILITY IN SPLUNK ENTERPRISE AND SPLUNK SECURE GATEWAY APP

Vairav CVE Report

Date: March 27, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

This report comprehensively analyzes two critical vulnerabilities affecting Splunk Enterprise and the Splunk Secure Gateway App. These vulnerabilities expose systems to remote code execution and sensitive information disclosure, significantly compromising security. CVE-2025-20229 allows unauthorized remote code execution due to insufficient authorization checks, while CVE-2025-20231 permits unauthorized access to sensitive session tokens. Organizations using vulnerable Splunk versions must immediately apply the recommended patches to mitigate potential risks and prevent exploitation.

VULNERABILITY DETAILS

CVE-2025-20229: Remote Code Execution through File Upload

Description: In Splunk Enterprise versions below 9.3.3, 9.2.5, and 9.1.8, and Splunk Cloud Platform versions below 9.3.2408.104, 9.2.2406.108, 9.2.2403.114, and 9.1.2312.208, a low-privileged user without "admin" or "power" roles can achieve Remote Code Execution (RCE) by uploading files to the $SPLUNK_HOME/var/run/splunk/apptemp directory due to missing authorization checks.

Impact: Arbitrary code execution, system compromise, data exfiltration, and service disruptions.

CVSS Score: 8.0 (High)

CVE-2025-20231: Sensitive Information Disclosure in Splunk Secure Gateway App

Description: In Splunk Enterprise versions below 9.4.1, 9.3.3, 9.2.5, and 9.1.8, and Splunk Secure Gateway App versions below 3.8.38 and 3.7.23, a low-privileged user could run searches using the permissions of higher-privileged users. The vulnerability is due to user session and authorization tokens being logged in clear text in splunk_secure_gateway.log.

Impact: Access to session tokens, impersonate privileged users, and exfiltrate sensitive data.

CVSS Score: 7.1 (High)

AFFECTED VERSIONS

Splunk Enterprise:

- 9.4 (9.4.0) – Fixed in 9.4.1
- 9.3 (9.3.0 to 9.3.2) – Fixed in 9.3.3
- 9.2 (9.2.0 to 9.2.4) – Fixed in 9.2.5
- 9.1 (9.1.0 to 9.1.7) – Fixed in 9.1.8

Splunk Cloud Platform:

- 9.3.2408 (9.3.2408.100 to 9.3.2408.103) – Fixed in 9.3.2408.104
- 9.2.2406 (9.2.2406.100 to 9.2.2406.107) – Fixed in 9.2.2406.108
- 9.2.2403 (Below 9.2.2403.113) – Fixed in 9.2.2403.114
- 9.1.2312 (Below 9.1.2312.207) – Fixed in 9.1.2312.208

Splunk Secure Gateway App:

- 3.8 (Below 3.8.38) – Fixed in 3.8.38
- 3.7 (Below 3.7.23) – Fixed in 3.7.23

EXPLOIT DETAILS

- **CVE-2025-20229:** Attackers exploit vulnerability by uploading malicious payloads to the specified directory, which are then executed by Splunk processes. This can be automated using publicly available scripts or modified to evade detection.
- **CVE-2025-20231:** Exploitation involves reading log files to retrieve session tokens, which can then be used to escalate privileges or access restricted data.

RECOMMENDATIONS

Patch & Upgrade:

- Upgrade to the latest versions of Splunk Enterprise and Splunk Secure Gateway App to mitigate these vulnerabilities.
- If upgrading is not immediately feasible, disable the Splunk Secure Gateway App as a temporary mitigation for CVE-2025-20231.

Mitigation Measures:

- Ensure proper access controls to restrict unauthorized file uploads.
- Regularly review and sanitize log files to prevent sensitive data exposure.

- Monitor for indicators of compromise (IoCs) associated with these vulnerabilities.
- Conduct security audits and penetration testing to assess system resilience.

REFERENCES

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

https://advisory.splunk.com/advisories/SVD-2025-0302

https://securityonline.info/splunk-alert-rce-and-data-leak-vulnerabilities-threaten-platforms/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com