مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Splunk Enterprise

Tracking #:432319111

Date:11-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Splunk has released security updates addressing several vulnerabilities affecting Splunk Enterprise and the Splunk Secure Gateway application including a critical vulnerability.

TECHNICAL DETAILS:

Splunk has released security updates addressing several high-severity vulnerabilities affecting Splunk Enterprise and the Splunk Secure Gateway application. The most critical vulnerability, CVE-2026-20253 (CVSS 9.8), allows unauthenticated attackers to perform arbitrary file creation and truncation operations through a vulnerable PostgreSQL sidecar service endpoint.

Vulnerability Details:

1. CVE-2026-20253 — Critical (CVSS 9.8) — Unauthenticated Arbitrary File Creation and Truncation
2. CVE-2026-20251 — High (CVSS 8.8) — Remote Code Execution via Unsafe Deserialization
3. CVE-2026-20252 — High (CVSS 7.6) — Server-Side Request Forgery (SSRF)
4. CVE-2026-20258 — High (CVSS 7.1) — Stored Cross-Site Scripting (XSS)

Note: Refer to the Splunk advisory for release notes and additional information.

Fixed Versions:

Splunk Enterprise

- Splunk Enterprise 10.4.0
- Splunk Enterprise 10.2.4
- Splunk Enterprise 10.0.7
- Splunk Enterprise 9.4.12
- Splunk Enterprise 9.3.13

Splunk Cloud Platform

- 10.3.2512.12
- 10.2.2510.15
- 10.1.2507.23
- 9.3.2411.132

Splunk Secure Gateway

- 3.10.6
- 3.9.20
- 3.8.67

RECOMMENDATIONS:

Immediate Actions:

- Upgrade affected Splunk Enterprise instances to a patched version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://advisory.splunk.com/