مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-Splunk Enterprise & DB Connect

Tracking #:432318444

Date:23-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Splunk has released a coordinated set of security advisories addressing multiple high-severity vulnerabilities in Splunk Enterprise for Windows and Splunk DB Connect.

TECHNICAL DETAILS:

Splunk has released a coordinated set of security advisories addressing multiple high-severity vulnerabilities in Splunk Enterprise for Windows and Splunk DB Connect. The most critical findings involve two Local Privilege Escalation (LPE) vulnerabilities — one via DLL search-order hijacking (CVE-2026-20140) and one via Python module search path abuse (CVE-2026-20143) — both of which could allow a low-privileged local user to execute arbitrary code with SYSTEM-level privileges upon service restart. Additionally, Splunk has addressed multiple high and critical severity vulnerabilities in third-party packages bundled with Splunk Enterprise and Splunk DB Connect, including issues in golang, OpenSSL, Node.js, aiohttp, urllib3, and qs.

Vulnerability Details
1. CVE-2026-20140 — LPE via DLL Search-Order Hijacking

- **CVSSv3.1 Score:** 7.7 (High)
- **CWE:** CWE-427 (Uncontrolled Search Path Element)

Affected Versions:

- Splunk Enterprise 10.0.0 to 10.0.2 → Fixed in 10.0.3
- Splunk Enterprise 9.4.0 to 9.4.7 → Fixed in 9.4.8
- Splunk Enterprise 9.3.0 to 9.3.8 → Fixed in 9.3.9
- Splunk Enterprise 9.2.0 to 9.2.11 → Fixed in 9.2.12
- Splunk Enterprise 10.2.x → Not affected

2. CVE-2026-20143 — LPE via Python Module Search Path

- **CVSSv3.1 Score:** 7.7 (High)
- **CWE:** CWE-427 (Uncontrolled Search Path Element)

Affected Versions:

- Splunk Enterprise 10.0.0 to 10.0.2 → Fixed in 10.0.3
- Splunk Enterprise 9.4.0 to 9.4.7 → Fixed in 9.4.8
- Splunk Enterprise 9.3.0 to 9.3.8 → Fixed in 9.3.9
- Splunk Enterprise 10.2.x → Not affected

3. SVD-2026-0211 — Third-Party Package CVEs in Splunk Enterprise
Fixed in: Splunk Enterprise 10.0.3, 9.4.8, 9.3.9, 9.2.12 and higher

- **golang** — Upgraded to 1.24.11 | Multiple CVEs | **Severity: Critical**
- **Node.js** (two separate components) — See vendor notes | Multiple CVEs | **Severity: High**
- **aiohttp** — Upgraded to 3.12.14 | CVE-2025-53643 | **Severity: High**
- **OpenSSL** — Upgraded to 1.0.2zm and 3.0.18 | CVE-2025-9230 | **Severity: High**

4. SVD-2026-0212 — Third-Party Package CVEs in Splunk DB Connect
Fixed in: Splunk DB Connect 4.2.0 and higher

- **qs** (query string parser) — Upgraded to 6.14.1 | CVE-2025-15284 | **Severity: Low**
- **urllib3** — Upgraded to 2.6.3 | CVE-2026-21441 | **Severity: High**

RECOMMENDATIONS:

- Upgrade all Splunk Enterprise for Windows deployments and Splunk DB Connect to the appropriate fixed 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/