AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Përditësime Sigurie – Splunk Enterprise & DB Connect

Data: 23/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Splunk ka publikuar një seri njoftimesh sigurie që adresojnë dobësi të shumta me rrezikshmëri të lartë në Splunk Enterprise për Windows dhe Splunk DB Connect. Gjetjet më kritike përfshijnë dy dobësi **Local Privilege Escalation (LPE)** — njëra përmes manipulimit të rendit të kërkimit të DLL-ve (CVE-2026-20140) dhe tjetra përmes abuzimit me path-in e kërkimit të moduleve Python (CVE-2026-20143) — të cilat mund t'i lejojnë një përdoruesi lokal me privilegje të ulëta të ekzekutojë kod arbitrar me privilegje të nivelit **SYSTEM** pas rinisjes së shërbimit.
Përveç kësaj, Splunk ka adresuar edhe dobësi të shumta me rrezikshmëri të lartë dhe kritike në paketat e palëve të treta të përfshira në Splunk Enterprise dhe Splunk DB Connect, duke përfshirë çështje në golang, OpenSSL, Node.js, aiohttp, urllib3 dhe qs.

Informacione Teknike

Detaje të Dobësive:

1. CVE-2026-20140 — LPE përmes manipulimit të rendit të kërkimit të DLL

- CVSSv3.1 Score: 7.7 (High)
- CWE: CWE-427 (Element i pakontrolluar në path kërkimi)

Versionet e prekura:

- Splunk Enterprise 10.0.0 – 10.0.2 → Rregulluar në 10.0.3
- Splunk Enterprise 9.4.0 – 9.4.7 → Rregulluar në 9.4.8
- Splunk Enterprise 9.3.0 – 9.3.8 → Rregulluar në 9.3.9
- Splunk Enterprise 9.2.0 – 9.2.11 → Rregulluar në 9.2.12
- Splunk Enterprise 10.2.x → Nuk preket

2. CVE-2026-20143 — LPE përmes path-it të kërkimit të moduleve Python

- CVSSv3.1 Score: 7.7 (High)
- CWE: CWE-427 (Element i pakontrolluar në path kërkimi)

Versionet e prekura:

- Splunk Enterprise 10.0.0 – 10.0.2 → Rregulluar në 10.0.3
- Splunk Enterprise 9.4.0 – 9.4.7 → Rregulluar në 9.4.8
- Splunk Enterprise 9.3.0 – 9.3.8 → Rregulluar në 9.3.9
- Splunk Enterprise 10.2.x → Nuk preket

3. SVD-2026-0211 — CVE në paketa të palëve të treta në Splunk Enterprise
Rregulluar në: Splunk Enterprise 10.0.3, 9.4.8, 9.3.9, 9.2.12 dhe më të reja

- golang — përditësuar në 1.24.11 | Dobësi të shumta | Rrezikshmëri: Kritike
- Node.js (dy komponentë të veçantë) — shih shënimet e prodhuesit | Dobësi të shumta | Rrezikshmëri: E lartë
- aiohttp — përditësuar në 3.12.14 | CVE-2025-53643 | Rrezikshmëri: E lartë
- OpenSSL — përditësuar në 1.0.2zm dhe 3.0.18 | CVE-2025-9230 | Rrezikshmëri: E lartë

4. SVD-2026-0212 — CVE në paketa të palëve të treta në Splunk DB Connect
Rregulluar në: Splunk DB Connect 4.2.0 dhe më të reja

- qs (parser query string) — përditësuar në 6.14.1 | CVE-2025-15284 | Rrezikshmëri: E ulët
- urllib3 — përditësuar në 2.6.3 | CVE-2026-21441 | Rrezikshmëri: E lartë

Rekomandime

Rekomandohet të përditësoni të gjitha instalimet Splunk Enterprise për Windows dhe Splunk DB Connect në versionet e rregulluara përkatëse.

Referenca

https://advisory.splunk.com/