مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-Splunk

Tracking #:432317770

Date:02-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Splunk has released security advisories addressing six vulnerabilities across Splunk Enterprise and Splunk Cloud Platform.

TECHNICAL DETAILS:

Splunk has released security advisories addressing six vulnerabilities across Splunk Enterprise and Splunk Cloud Platform. The flaws affect multiple components, including job execution, saved searches, dashboards, LDAP authentication, and Splunk's web interface.

The most critical issue, CVE-2025-20371, is an unauthenticated blind server-side request forgery (SSRF) with a CVSS score of 7.5. Successful exploitation could allow attackers to perform REST API calls on behalf of high-privileged users, leading to data exposure, privilege escalation, or lateral movement within enterprise environments.
Other vulnerabilities include reflected and stored XSS, improper access control, XML external entity (XXE) injection, and denial-of-service via LDAP bind abuse. While several require low-privileged or authenticated access, the SSRF flaw is exploitable without authentication under certain configurations, making it the most severe.

Vulnerability Details:

1. **CVE-2025-20366 – Improper Access Control (CVSS 6.5)**
   - **Impact:** Low-privileged users can retrieve sensitive search results by guessing background job Search IDs (SIDs).
   - **Fix:** Upgrade to patched versions.

2. **CVE-2025-20367 – Reflected XSS (CVSS 5.7)**
   - **Impact:** Attackers can inject JavaScript payloads via /app/search/table endpoint (dataset.command parameter).
   - **Fix:** Apply vendor patches.

3. **CVE-2025-20368 – Stored XSS in Saved Searches (CVSS 5.7)**
   - **Impact:** Malicious payloads embedded in error messages or job inspection details persistently execute across users.
   - **Fix:** Upgrade to patched versions.

4. **CVE-2025-20369 – XML External Entity (XXE) Injection (CVSS 4.6)**
   - **Impact:** Exploitable via dashboard tab labels; can be abused for DoS via XXE payloads.
   - **Fix:** Upgrade to 9.4.4 or higher.

5. **CVE-2025-20370 – DoS via Multiple LDAP Bind Requests (CVSS 4.9)**
   - **Impact:** High CPU usage and potential instance crash if attackers abuse change_authentication capability.
   - **Fix:** Patch or remove risky capability from user roles.

6. **CVE-2025-20371 – Unauthenticated Blind SSRF (CVSS 7.5)**
   - **Impact:** Allows unauthenticated attackers to trigger SSRF and perform REST API calls on

behalf of privileged users.

- **Preconditions:** enableSplunkWebClientNetloc must be enabled. Likely requires phishing to initiate.
- **Fix:** Patch to latest versions, or disable enableSplunkWebClientNetloc.

Fixed Versions:

- **Splunk Enterprise:** 10.0.1, 9.4.4, 9.3.6, or 9.2.8
- **Splunk Cloud Platform:** Apply the latest hotfixes as deployed by Splunk

RECOMMENDATIONS:

- Immediate Patching - Organizations using Splunk must apply vendor patches immediately to mitigate these threats and reduce exposure.

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.

REFERNCES:

- https://advisory.splunk.com//advisories