GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

31 August 2026

Advisory 215: Splunk Enterprise Multiple SPL Injection Vulnerabilities (CVE-2026-76254, CVE-2026-76255, CVE-2026-76322, CVE-2026-76323).

Release Date: 24th August 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate Splunk Enterprise. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-76254, CVE-2026-76255, CVE-2026-76322 and CVE-2026-76323 are Search Processing Language (SPL) injection vulnerabilities in Splunk Enterprise. Each allows SPL safeguards designed to stop risky, attacker-controlled searches from being bypassed through a different Splunk feature: the Dataset Explorer, the Data Model Editor, Dashboard Studio dashboards, and Job Details dashboard links respectively.

The most severe, CVE-2026-76254 (CVSS 7.5), lets an unauthenticated user manipulate dataset names to dispatch arbitrary SPL pipelines without the normal safeguards, potentially exposing sensitive indexed data. The remaining three require an authenticated but low-privileged user, and in most cases a social-engineering step such as getting another user to open a crafted dashboard or link, to run attacker-controlled SPL in the context of a more privileged user.

What are the systems affected?

The following version(s) are affected (all four CVEs):

- Splunk Enterprise 10.4.0 – 10.4.1 – (Affected)
- Splunk Enterprise 10.2.0 – 10.2.5, 10.0.0 – 10.0.8, and 9.4.0 – 9.4.13 – (Affected)

Splunk Enterprise 10.4.2, 10.2.6, 10.0.9 and 9.4.14 and later are not affected (patched).

Administrators should check their installed Splunk Enterprise version against the fixed versions above and refer to Splunk's August 2026 Security Hardening Release (SVD-2026-0801) for the full advisory covering all four CVEs.

What does this mean?

Typical attack flow:

1. **Reach a vulnerable SPL entry point**
    - An attacker (unauthenticated for CVE-2026-76254, or a low-privileged authenticated user for the others) interacts with Dataset Explorer, the Data Model Editor, a Dashboard Studio dashboard, or a Job Details link.
2. **Bypass SPL safeguards**
    - Crafted input causes Splunk to dispatch or execute SPL commands that the platform's risky-command safeguards were meant to block, without further authorization checks.

Attack vectors:

- Direct, unauthenticated manipulation of dataset names (CVE-2026-76254).
- Social engineering of a victim user into opening a crafted Data Model Editor object, Dashboard Studio dashboard, or Job Details link (CVE-2026-76255, CVE-2026-76322, CVE-2026-76323).

Successful exploitation may allow attackers to:

- Access indexed data the attacker would not otherwise be authorized to search.
- Run SPL commands in the context of a higher-privileged user who views a crafted dashboard or link.

Mitigation process

CERTVU recommends the following:

1. Upgrade Splunk Enterprise

- Upgrade to Splunk Enterprise 10.4.2, 10.2.6, 10.0.9 or 9.4.14 (or later on the same major/minor line), per Splunk's August 2026 Security Hardening Release (SVD-2026-0801).

2. Apply least privilege
3. Audit dashboards and datasets

- Review existing Dataset Explorer entries, Data Model Editor objects, Dashboard Studio dashboards and saved Job Details links for unexpected or attacker-supplied SPL before and after patching.

4. User awareness

- Caution users against opening dashboards or links from untrusted or unexpected sources, since three of the four flaws require this kind of interaction to exploit.

5. Monitor Splunk's security advisories page for further updates

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://advisory.splunk.com/advisories/SVD-2026-0801
2. https://www.cve.org/CVERecord?id=CVE-2026-76254
3. https://www.cve.org/CVERecord?id=CVE-2026-76255
4. https://www.cve.org/CVERecord?id=CVE-2026-76322
5. https://www.cve.org/CVERecord?id=CVE-2026-76323