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

1 September 2026

Advisory 218: Splunk Enterprise for Windows Local Privilege Escalation Vulnerability (CVE-2026-76259).

Release Date: 31st August 2026
Impact: CRITICAL
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 on Windows hosts. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-76259 is a local privilege escalation vulnerability in Splunk Enterprise for Windows. It allows a local user with access to the Windows host to bind to Splunk's management port before the Splunk service starts, then intercept authentication tokens from child processes as they start up.

The root cause is that the Windows management-port listener does not apply exclusive address-binding protections before the service starts, leaving a window in which another local process can claim the port. An attacker who captures these tokens can use them to compromise the integrity and confidentiality of all data and services managed by that Splunk instance.

What are the systems affected?

The following version(s) are affected:

- Splunk Enterprise for Windows below 10.4.2, 10.2.6, 10.0.9, 9.4.13 and 9.3.14 - (Affected)

Splunk Enterprise for Windows 10.4.2, 10.2.6, 10.0.9, 9.4.13, 9.3.14 and later - (Not affected, patched)

This vulnerability affects the Windows build of Splunk Enterprise only; Splunk Enterprise on Linux/Unix hosts is not affected. Administrators should verify their installed version and platform against Splunk's August 2026 Security Hardening Release (SVD-2026-0801).

What does this mean?

Typical attack flow:

1. **Race the management-port listener**
    - A local user or process on the Windows host binds to Splunk's management port before the Splunk service itself starts and claims it.
2. **Intercept authentication tokens**
    - As Splunk child processes start up and attempt to authenticate to the management port, the attacker-controlled listener captures their tokens.

Attack vectors:

- Local access to the Windows host running Splunk Enterprise (no remote network exploitation).
- Timing the local process to bind the management port ahead of the Splunk service, e.g. at host boot or service restart.

Successful exploitation may allow attackers to:

- Obtain valid Splunk authentication tokens without needing existing Splunk credentials.
- Use those tokens to compromise the confidentiality and integrity of all data and system functions the Splunk instance manages.

Mitigation process

CERTVU recommends the following:

1. Upgrade Splunk Enterprise for Windows

- Upgrade to Splunk Enterprise for Windows 10.4.2, 10.2.6, 10.0.9, 9.4.13, 9.3.14 or later, per Splunk's August 2026 Security Hardening Release (SVD-2026-0801).

2. Apply least privilege on the host
3. Restrict local logon rights

- Limit which accounts can log on locally or run processes on the Windows host running Splunk Enterprise, since exploitation requires local access.

4. Audit the estate for the affected product

- Identify every Windows host running Splunk Enterprise and confirm each is patched or scheduled for patching.

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-2026-76259