مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Splunk Enterprise

Tracking #:432318578
Date:12-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Splunk Enterprise that could allow the execution of arbitrary commands on affected systems.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in Splunk Enterprise that could allow the execution of arbitrary shell commands through a REST API endpoint. The issue occurs due to insufficient input sanitization when previewing uploaded files before indexing.

Vulnerability Details

- **CVE:** CVE-2026-20163
- **Severity:** High (CVSS 3.1 Score: 8.0)
- A remote command execution vulnerability exists in the /splunkd/__upload/indexing/preview REST endpoint in Splunk Enterprise and Splunk Cloud Platform. A user with a role containing the high-privilege capability **edit_cmd** may exploit the **unarchive_cmd** parameter to execute arbitrary shell commands. This occurs due to improper input validation when processing uploaded files during the indexing preview process.

Affected Versions

- Splunk Enterprise versions below 10.2.0, 10.0.4, 9.4.9, and 9.3.10
- Splunk Cloud Platform versions below 10.2.2510.5, 10.0.2503.12, 10.1.2507.16, and 9.3.2411.124

Fixed Versions

- Splunk Enterprise versions 10.2.0, 10.0.4, 9.4.9, 9.3.10 or later
- Splunk Cloud Platform versions 10.2.2510.5, 10.0.2503.12, 10.1.2507.16, 9.3.2411.124 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Splunk.

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/advisories/SVD-2026-0302