مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Splunk Products

Tracking #:432316024

Date:05-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Splunk released security updates to address several vulnerabilities in their products.

TECHNICAL DETAILS:

Splunk addressed 16 vulnerabilities in Splunk Enterprise and Cloud Platform including six high-severity bugs. Three of the high-severity issues are remote code execution flaws that require authentication for successful exploitation.

Remote Code Execution (RCE):

- **CVE-2024-36985** (Splunk Enterprise versions 9.2.x, 9.1.x, and 9.0.x) - Exploitable by low-privileged user, mitigated by disabling 'splunk_archiver' application. Patched in versions 9.2.2, 9.1.5, and 9.0.10.
- **CVE-2024-36984** (Splunk Enterprise for Windows) - Requires use of 'collect' SPL command.
- Dashboard PDF generation (Enterprise & Cloud Platform) - Due to vulnerable ReportLab Toolkit library (v3.6.1)

Splunk also patched a high-severity command injection flaw that could allow an authenticated user to inject and execute commands within a privileged context. The remaining high-severity bugs include a path traversal in Splunk Enterprise on Windows and a denial-of-service in the Enterprise and Cloud Platform products. Splunk has not reported any of these vulnerabilities being actively exploited in the wild.

Fixed Versions:

- Splunk Enterprise versions 9.2.2, 9.1.5, and 9.0.10, or higher.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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