مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

High Severity Vulnerability in Splunk Enterprise

Tracking #:432316073

Date:22-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a path traversal vulnerability in Splunk Enterprise that allows attackers to potentially read unauthorized files on the Splunk server, potentially leading to data breaches.

TECHNICAL DETAILS:

A High Severity path traversal vulnerability (CVE-2024-36991) identified in Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 that allows attackers to potentially read unauthorized files on the Splunk server, potentially leading to data breaches.

- **Vulnerability: CVE-2024-36991** (CVSSv3 score: 7.5 - high severity)
- **Type:** Path Traversal Vulnerability (CWE-35)
- **Affected Software:** Splunk Enterprise Windows versions below 9.2.2, 9.1.5, and 9.0.10
- **Impact:** Successful exploitation could allow attackers to read sensitive information stored on the Splunk server.
- **Exploit Availability:** Proof-of-concept exploit code is publicly available.
- **Affected Systems:** This vulnerability only affects Splunk Enterprise with Splunk Web enabled.

Fixed Versions:

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

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Splunk Enterprise to the fixed version at the earliest.

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-2024-0711