مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in Splunk Secure Gateway App

Tracking #:432316625

Date:12-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability has been identified in the Splunk Secure Gateway app that could allow low-privileged users to execute arbitrary code on vulnerable systems, leading to potential remote code execution (RCE).

TECHNICAL DETAILS:

A high severity vulnerability (CVE-2024-53247) has been identified in the Splunk Secure Gateway app that could allow low-privileged users to execute arbitrary code on vulnerable systems, leading to potential remote code execution (RCE).

Details of the Vulnerability:

- **Vulnerability Identifier:** CVE-2024-53247
- **CVSS Score:** 8.8 (High)
- **Affected Products:**
  - **Splunk Enterprise:** Versions below 9.3.2, 9.2.4, and 9.1.7
  - **Splunk Secure Gateway App:** Versions below 3.2.461 and 3.7.13 on Splunk Cloud Platform
- **Vulnerability Description:**
- The vulnerability arises from an unsafe deserialization of data caused by an insecure use of the jsonpickle Python library within the Splunk Secure Gateway app. This flaw enables attackers to inject arbitrary code that can be executed remotely on the affected system. Successful exploitation of this issue allows attackers to compromise the integrity of the system, potentially leading to system takeover and remote code execution.

Fixed versions:

- Splunk Enterprise to versions 9.3.2, 9.2.4, and 9.1.7, or higher
- Splunk Secure Gateway App 3.7.13, 3.2.461

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the patched versions 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-2024-1205