مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Splunk Products

Tracking #:432316394

Date:15-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Splunk has released security updates addressing multiple vulnerabilities in Splunk Enterprise and Splunk Cloud Platform. Notably, these vulnerabilities include several high-severity flaws that could lead to remote code execution (RCE) and unauthorized access for low-privileged users.

Critical Remote Code Execution (RCE) Vulnerabilities

- CVE-2024-45731: Affects Windows installations where Splunk Enterprise is installed on a separate disk. Attackers could potentially write malicious DLL files to the Windows system root directory, leading to system compromise.
- CVE-2024-45733: Results from insecure session storage configuration. This vulnerability affects Splunk Enterprise for Windows versions below 9.2.3 and 9.1.6.

Unauthorized Access by Low-Privilege Users

- CVE-2024-45732: Allows low-privileged users to run searches as the "nobody" user within the SplunkDeploymentServerConfig app, risking exposure of restricted data.
- CVE-2024-45734: Enables unauthorized users to view images on the host machine.
- CVE-2024-45735: Grants access to sensitive configuration data in the Splunk Secure Gateway App.
- CVE-2024-45736: Allows low-privileged users to crash the Splunk daemon.
- CVE-2024-45737: Enables manipulation of the maintenance mode state of the App Key Value Store.

Information Disclosure and Cross-Site Scripting (XSS)

- CVE-2024-45738 & CVE-2024-45739: These vulnerabilities could lead to sensitive information disclosure.
- CVE-2024-45740 & CVE-2024-45741: Persistent XSS vulnerabilities that could be exploited to inject malicious scripts into web pages viewed by other users.

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/