مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Cisco Products

Tracking #:432316067

Date:18-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco released security updates to address multiple vulnerabilities in various products.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-20419**- Severity: Critical, CVSS Score: Base 10.0
  - A vulnerability in the authentication system of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to change the password of any user, including administrative users
  - Affected Product-Cisco SSM On-Prem and Cisco Smart Software Manager Satellite (SSM Satellite).

- **CVE-2024-20435**- Severity: High, CVSS Score: Base 8.8
  - A vulnerability in the CLI of Cisco AsyncOS for Secure Web Appliance could allow an authenticated, local attacker to execute arbitrary commands and elevate privileges to root.
  - Affected Product- Cisco AsyncOS for Secure Web Appliance, both virtual and hardware appliances.

- **CVE-2024-20323**- Severity: High, CVSS Score: Base 7.5
  - A vulnerability in Cisco Intelligent Node (iNode) Software could allow an unauthenticated, remote attacker to hijack the TLS connection between Cisco iNode Manager and associated intelligent nodes and send arbitrary traffic to an affected device.
  - Affected Product- Cisco iNode Software and Cisco iNode Manager Software.

- **CVE-2024-20296**- Severity: High, CVSS Score: Base 4.7
  - A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to upload arbitrary files to an affected device. To exploit this vulnerability, an attacker would need at least valid Policy Admin credentials on the affected device.
  - Affected Product- Cisco ISE in the default configuration.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends referring the patch update advisory released by Cisco and applying the relevant patches as early as possible.

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-priv-esc-7uHpZsCC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-inode-static-key-VUVCeynn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-upload-krW2TxA9