مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Cisco Products

Tracking #:432316076

Date:22-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco released security updates to address a critical vulnerability in their product.

TECHNICAL DETAILS:

A vulnerability in the content scanning and message filtering features of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to overwrite arbitrary files on the underlying operating system.

Vulnerability Details:

- **CVE-2024-20401** | CVSS v3: 9.8 – Critical
  - This vulnerability is due to improper handling of email attachments when file analysis and content filters are enabled. An attacker could exploit this vulnerability by sending an email that contains a crafted attachment through an affected device.
  - A successful exploit could allow the attacker to replace any file on the underlying file system. The attacker could then perform any of the following actions: add users with root privileges, modify the device configuration, execute arbitrary code, or cause a permanent denial of service (DoS) condition on the affected device.

Affected Versions:

- This vulnerability affects Cisco Secure Email Gateway if it is running a vulnerable release of Cisco AsyncOS and both of the following conditions are met:
  - Either the file analysis feature, which is part of Cisco Advanced Malware Protection (AMP), or the content filter feature is enabled and assigned to an incoming mail policy
  - The Content Scanner Tools version is earlier than 23.3.0.4823

Fixed Version:

- Content Scanner Tools version 23.3.0.4823 and later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Cisco.

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-esa-afw-bGG2UsjH