مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Cisco Finesse

Tracking #:432315932

Date:06-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Cisco Finesse that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

CVE-2024-20404: Cisco Finesse SSRF Vulnerability

- **CVSS Base Score:** 7.2 (High)
- A vulnerability in the Cisco Finesse web-based management interface allows unauthenticated remote attackers to conduct a Server-Side Request Forgery (SSRF) attack. This vulnerability arises due to insufficient validation of user-supplied input within specific HTTP requests.
- A successful exploit could grant attackers access to limited sensitive information associated with services on the affected system.

CVE-2024-20405: Cisco Finesse Stored XSS through RFI Vulnerability

- **CVSS Base Score:** 4.8 (Medium)
- A vulnerability in the Cisco Finesse web-based management interface allows unauthenticated remote attackers to launch a stored XSS attack by exploiting a Remote File Inclusion (RFI) vulnerability. This vulnerability exists due to insufficient validation of user-supplied input within specific HTTP requests.
- A successful exploit could allow attackers to execute arbitrary script code in the context of the affected interface or potentially access sensitive information on the affected device by tricking a user into clicking a malicious link.

Affected Products:

These vulnerabilities affected Cisco Finesse in the default configuration.

The following Cisco products that may be bundled with Cisco Finesse are also affected by these vulnerabilities:

- Packaged Contact Center Enterprise (Packaged CCE)
- Unified Contact Center Enterprise (Unified CCE)
- Unified Contact Center Express (Unified CCX)
- Unified Intelligence Center

Affected Version	Fixed Version
11.6(1) ES11 and earlier	Migrate to a fixed release.
12.6(2) ES01 and earlier	12.6(2) ES03

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions 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-finesse-ssrf-rfi-Um7wT8Ew