

مجلس الأمان السيبراني CYBER SECURITY COUNCIL



Security Updates - Cisco
Tracking #:432317496
Date:17-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco released security updates, addressing a vulnerability in its web-based management interface of Cisco Unified Intelligence Center. The vulnerability could allow an authenticated, remote attacker to upload arbitrary files to an affected device.

TECHNICAL DETAILS:

This vulnerability is due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit this vulnerability by uploading arbitrary files to an affected device.

A successful exploit could allow the attacker to store malicious files on the system and execute arbitrary commands on the operating system. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could elevate privileges to root. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Report Designer.

Vulnerability Details:

- CVE ID: CVE-2025-20274
- Base Score: 6.3
- Severity: Medium
- Workarounds: N/A
- Advisory ID: cisco-sa-cuis-file-upload-UhNEtStm

Affected Versions:

This vulnerability affects **Cisco Unified Intelligence Center**, regardless of device configuration, including if it is being used as part of the following Cisco solutions:

- Packaged Contact Center Enterprise (Packaged CCE)
- Unified Contact Center Enterprise (Unified CCE)

This vulnerability also affects **Cisco Unified Contact Center Express (Unified CCX)** because it includes Cisco Unified Intelligence Center as part of its software bundle.

Fixed Versions:

Cisco Unified Intelligence Center Release	First Fixed Release
12.5	12.5(1) SU ES05
12.6	12.6(2) ES05
15	Not vulnerable.

Cisco Unified CCX Release	First Fixed Release
12.5(1) SU3 and earlier	Migrate to a fixed release.
15	Not vulnerable.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates 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-cuis-file-upload-UhNEtStm>