مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Cisco Unified CCX

Tracking #:432317951

Date:06-11-2025

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco has released emergency patches addressing two critical remote code execution (RCE) vulnerabilities in Cisco Unified Contact Center Express (Unified CCX).

TECHNICAL DETAILS:

Cisco has released emergency patches addressing two critical remote code execution (RCE) vulnerabilities in Cisco Unified Contact Center Express (Unified CCX). These flaws can be exploited without authentication and allow remote attackers to gain root-level access or administrative control over affected systems.

The vulnerabilities — CVE-2025-20354 and CVE-2025-20358 — impact core Unified CCX components, specifically the Java Remote Method Invocation (RMI) process and the CCX Editor scripting tool. Successful exploitation could enable attackers to fully compromise Unified CCX servers used in enterprise call centers, execute arbitrary commands, manipulate configurations, or install persistent malware.

Vulnerability Details
1. CVE-2025-20354 – Java RMI Remote Code Execution (CVSS 9.8, Critical)
Description:
A critical flaw exists in the Java RMI process of Cisco Unified CCX due to improper authentication and file handling mechanisms. A remote, unauthenticated attacker could exploit this by sending a specially crafted RMI request to an exposed CCX instance.

2. CVE-2025-20358 – CCX Editor Authentication Bypass (CVSS 9.4, Critical)
Description:
A vulnerability in the CCX Editor component allows attackers to bypass authentication by exploiting improper validation in the communication between the Editor client and the Unified CCX server.
Attackers can redirect the authentication process to a malicious server, forging authentication responses that grant administrative permissions within the scripting environment. This access enables attackers to create, modify, and execute scripts on the target CCX server with elevated privileges.

Patched Versions:

- Unified CCX 12.5 SU3 ES07
- Unified CCX 15.0 ES01

RECOMMENDATIONS:

- Organizations are strongly advised to apply Cisco's security updates immediately and conduct a thorough review of exposed Unified CCX instances.

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-cc-unauth-rce-QeN8h7mQ