Critical Cisco Unified Contact Center Express Remote Code Execution Vulnerabilities

TL;DR

Two critical vulnerabilities (CVE-2025-20354 and CVE-2025-20358) in Cisco Unified Contact Center Express (Unified CCX) could allow unauthenticated attackers to execute arbitrary code or bypass authentication.

There are no workarounds and it's recommended that customers apply the fixed releases immediately.

Overview

There are two critical vulnerabilities ((CVE-2025-20354 and CVE-2025-20358) in the Cisco's Java Remote Method Invocation (RMI) process and CCX Editor components of Unified Contact Center Express (Unified CCX). If exploited, these flaws could let remote attackers upload arbitrary files, execute commands with root privileges, or bypass authentication to gain admin-level access for script creation and execution.

Affected Products

- Cisco Unified CCX – All versions prior to the following fixed releases:
  - 12.5 SU3 and earlier – Fixed in 12.5 SU3 ES07
  - 15.0 – Fixed in 15.0 ES01

***Important Note**: Cisco confirmed that Packaged CCE and Unified CCE are not affected.*

Vulnerability Breakdown

- CVE-2025-20354 (CVSS 9.8) is in the Java RMI process of Unified CCX and results from improper authentication mechanisms tied to specific features. A remote attacker could upload a malicious file to the RMI process and execute arbitrary commands as root on the underlying operating system. Successful exploitation grants full control of the affected system.
- CVE-2025-20358 (CVSS 9.4) affects the CCX Editor application and stems from weak authentication between the editor and the Unified CCX server. An attacker could redirect authentication to a malicious server and trick the CCX Editor into granting access, allowing arbitrary script creation and execution on the system.

Both vulnerabilities can be exploited independently, and exploitation of one does not rely on the other. If these flaws are exploited, attackers could take over the CCX server, steal data, and shut down call-center operations. That kind of access could let them

move deeper into the network. Cisco has released security updates to address both vulnerabilities, and there are currently no reports of active exploitation. There are also no temporary workarounds available, therefore Aspire recommends patching immediately.

***Important Note**: It's worth noting that CVE-2025-20354 in Cisco Unified Contact Center Express should not be confused with CVE-2024-20354 in Cisco Aironet Access Points. The two share a similar CVE number but affect entirely different Cisco products.*

The earlier Aironet flaw has been exploited in maritime and logistics attacks, while Cisco has stated there's no evidence that the newly disclosed Unified CCX vulnerabilities have been used in the wild.

Aspire Protects

- **Patch** – Apply Cisco's patches for CVE-2025-20354 and CVE-2025-20358 immediately. See Cisco's advisory for more information.
- Do not expose Unified CCX servers directly to the internet. Restrict access to management interfaces to trusted networks only.
- Monitor for abnormal activity, including unknown files, unexpected scripts, or unusual administrative operations within Unified CCX environments.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] — The attacker may exploit the Java RMI process to upload a crafted file and gain initial code execution on the CCX host.

Execution

- Command and Scripting Interpreter [T1059] — The attacker may run uploaded scripts or commands to stage tools and execute payloads.

Credential Access

- Valid Accounts [T1078] — The attacker may create or misuse local/admin accounts or hijack editor workflows to maintain administrative access.

Collection

- Data from Information Repositories [T1213] — The attacker may harvest call recordings, configuration files, and PII stored on the CCX host.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Unified CCX is widely used in enterprise contact centers, meaning these vulnerabilities can impact any organization using Cisco's voice or call-center infrastructure, including:

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Unified Contact Center Express Remote Code Execution Vulnerabilities

Hacktivists, nation-state hackers target global maritime infrastructure as cyberattacks, GPS spoofing surge - Industrial Cyber