Cisco Contact Center & Cisco ISE Vulnerabilities

TL;DR

Cisco issued fixes for several medium-severity vulnerabilities across its Contact Center platforms (Unified CCX, Unified CCE, Packaged CCE, and CUIC) and Identity Services Engine (ISE).

All issues require valid credentials to exploit, but once an attacker is inside, they can read files, upload malicious content, run commands, elevate privileges, or trigger reflected XSS. No workarounds exist. Organizations should patch as soon as possible.

Overview

Cisco released updates for multiple vulnerabilities across its Contact Center product line and Cisco ISE. While none of these flaws can be exploited anonymously, they do give a logged-in attacker more access than they should ever have.

Vulnerability Breakdown

Unified Contact Center CCX / CCE / Packaged CCE / CUIC
All CCX vulnerabilities require valid administrative credentials but allow deep access once exploited.

- **CVE-2025-20375 (CVSS 6.5)** — Arbitrary File Upload
  The CCX web UI does not properly validate certain inputs, allowing an attacker with admin credentials to upload crafted files and run them on the appliance.
- **CVE-2025-20376 (CVSS 6.5)** — Remote Code Execution with Privilege Escalation
  Another input-handling flaw in the CCX file upload mechanism allows an authenticated attacker to run commands and escalate to root.
- **CVE-2025-20374 (CVSS 4.9)** — Arbitrary File Download via Directory Traversal
  Improper request validation lets an authenticated user pull files from the underlying OS they were never meant to view.
- **CVE-2025-20377 (CVSS 4.3)** — CUIC API Information Disclosure
  Weak request validation on certain CUIC API endpoints lets a low-privileged user retrieve data normally reserved for higher-level roles.

Cisco ISE and ISE-PIC are impacted by both reflected XSS and an information disclosure weakness. All issues require valid credentials.

- **CVE-2025-20289 (CVSS 4.8), CVE-2025-20303, CVE-2025-20304 (CVSS 5.4)** — Reflected XSS
  The ISE web interface does not properly sanitize user input, allowing attackers

with low-privileged accounts to inject malicious code into various pages. A successful attempt lets them run script code in another user's browser session.

- **CVE-2025-20305 (CVSS 4.3)** — Information Disclosure
  Certain sensitive files are not protected correctly, allowing a read-only admin to view data normally restricted to full administrators, including passwords.

If your organization relies on these platforms, patch as soon as possible and make sure nothing unusual has happened on the admin side before the updates.

Aspire Protects

- **Patch** – Patch all affected Unified CCX, CCE, Packaged CCE, and CUIC systems to the fixed versions published in Cisco's advisory.
  - Patch Guidance - CVE-2025-20374, CVE-2025-20375, CVE-2025-20376, CVE-2025-20377.
- **Patch** - Patch Cisco ISE to the fixed releases for reflected XSS and information disclosure issues.
  - Patch Guidance - CVE-2025-20289, CVE-2025-20303, CVE-2025-20304, CVE-2025-20305.
- Review administrative user lists and remove dormant or unnecessary accounts.
- Monitor for unusual file upload activity, privilege escalation attempts, or unexpected API calls.

TTPs to Watch

Execution

- Command Execution [T1059] – The attacker may run malicious files or commands after uploading them through the CCX web interface.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – The attacker may advance from an authenticated user to root-level access on affected CCX systems.

Collection

- Data from Local System [T1005] – The attacker may read files from the underlying OS by abusing the CCX directory traversal flaw.

Impact

- Manipulate Web Interfaces [T1605] – The attacker may inject script code into ISE's web interface through the reflected XSS issues.

IoCs

There are no known IoCs 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

The vulnerabilities affect any organization running Cisco Unified Contact Center or Cisco ISE:

- 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 Identity Services Engine Reflected Cross-Site Scripting and Information Disclosure Vulnerabilities

Multiple Cisco Contact Center Products Vulnerabilities