Cisco Software Vulnerabilities Affect Contact Center, Intersight, and IEC6400 Platforms

TL;DR

Cisco patched multiple medium-severity vulnerabilities affecting Contact Center Enterprise platforms, Intersight Virtual Appliances, and IEC6400 Edge Compute software.

The issues include cross-site scripting in Contact Center management interfaces, a local privilege escalation flaw in Intersight Virtual Appliances, and an SSH denial-of-service condition in IEC6400 systems.

CVEs: CVE-2026-20055, CVE-2026-20109, CVE-2026-20092, and CVE-2026-20080.

Overview

Cisco released security updates addressing four vulnerabilities (CVE-2026-20055, CVE-2026-20109, CVE-2026-20092, and CVE-2026-20080) impacting systems that are often deployed in trusted, high-access roles. The affected platforms include Contact Center Enterprise management interfaces, Intersight Virtual Appliances, and IEC6400 Wireless Backhaul Edge Compute Software.

While none of the vulnerabilities are known to be exploited in the wild, all require patching due to the lack of viable workarounds and the access levels involved. In several cases, exploitation depends on administrative access, but the resulting impact could extend beyond the initial user context.

CVE-2026-20055 and CVE-2026-20109 (CVSS 4.8) – Cisco Packaged CCE and Unified CCE Cross-Site Scripting

- These vulnerabilities affect the web-based management interface used by Cisco Contact Center platforms. Improper validation of user-supplied input allows an authenticated administrator to inject malicious script content into specific interface pages. Successful exploitation could lead to script execution within another user's browser session and exposure of browser-accessible management data.

CVE-2026-20092 (CVSS 6.0) – Cisco Intersight Virtual Appliance Privilege Escalation

- A flaw in file permissions within the read-only maintenance shell allows a local administrative user to escalate privileges to root. Once elevated, the attacker would gain full control of the virtual appliance, including access to sensitive configuration data and hosted workloads, with the potential to disrupt operations.

CVE-2026-20080 (CVSS 5.3) – Cisco IEC6400 SSH Denial of Service

- The SSH service in IEC6400 Edge Compute Software lacks sufficient flood protection. An unauthenticated remote attacker could overwhelm the SSH service, rendering it unavailable. While the issue does not impact other device functions, loss of SSH access could interfere with management and response efforts during an incident.

These vulnerabilities sit in management and infrastructure components that already have elevated trust. Leaving them unpatched keeps the door open for misuse. Although Cisco reported no public exploitation or malicious activity, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – Upgrade all affected Cisco products to the fixed releases listed in the advisories.
  - CVE-2026-20055, CVE-2026-20109, CVE-2026-20092, and CVE-2026-20080.
- Review administrative access to management interfaces and maintenance shells
- Disable unnecessary services, including SSH, where operationally feasible
- Monitor for abnormal activity tied to management access following patching

TTPs

Initial Access

- Valid Accounts [T1078] – The attacker logged in using valid administrative credentials to access affected management interfaces and maintenance shells.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker abused improper file permissions to escalate privileges from administrative access to root on the Intersight Virtual Appliance.

Impact

- Endpoint Denial of Service [T1499] – The attacker overwhelmed the SSH service on IEC6400 systems, making management access unavailable during the attack.

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

These Cisco enterprise software vulnerabilities affect organizations that rely on Contact Center platforms, infrastructure management appliances, or edge compute systems for daily operations.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- 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 Packaged Contact Center Enterprise and Cisco Unified Contact Center Enterprise Cross-Site Scripting Vulnerabilities
Cisco Intersight Virtual Appliance Privilege Escalation Vulnerability
Cisco IEC6400 Wireless Backhaul Edge Compute Software SSH Denial of Service Vulnerability