Cisco Patches 35 Vulnerabilities -Two Critical RCE Flaws Could Allow Full System Compromise

Overview

TL;DR

Cisco dropped fixes for 35 vulnerabilities this week, including two critical remote code execution flaws (CVE-2025-32433 and CVE-2025-20188) that allow unauthenticated attackers to gain full system control.

Devices running affected versions of Erlang/OTP SSH and IOS XE Wireless LAN Controllers are at risk. No workarounds exist, patches are the only option.

This week, Cisco released 35 security patches, including two critical vulnerabilities with CVSS scores of 10.0. The flaws impact a broad range of Cisco products, including IOS XE software, wireless controllers, and network orchestration platforms. Both vulnerabilities allow unauthenticated, remote code execution.

CVE-2025-32433 (CVSS 10) is a remote code execution flaw in the Erlang/OTP SSH server used across multiple Cisco products. It can be exploited without authentication during SSH message handling. Affected products include ConfD, NSO, and Ultra Cloud Core, with no workarounds in most cases. Proof-of-concept code is public, and patching is the only real fix.

CVE-2025-20188 (CVSS 10) is an arbitrary file upload vulnerability in IOS XE Wireless LAN Controllers. It stems from a hard-coded JWT in the Out-of-Band AP image download feature, which is disabled by default. If enabled, it allows unauthenticated attackers to upload malicious files and execute commands as root. Cisco has released patches, and disabling the feature is a temporary mitigation if patching can't be done right away.

Cisco's latest patch release includes two serious vulnerabilities that let attackers take control of affected systems. These are real world risks in widely deployed products. Patching as soon as possible is highly recommended.

Other Cisco Vulnerabilities

- CVE-2025-20186 (CVSS 8.8) – Command injection in IOS XE; requires authentication
- CVE-2025-20164 (CVSS 8.8) – Privilege escalation in IOS XE

- CVE-2025-20154 (CVSS 7.5) – DoS vulnerability exploitable without authentication
- CVE-2025-20182 (CVSS 7.5) – Additional unauthenticated DoS flaw
- CVE-2025-20162 (CVSS 7.5) – DoS attack via crafted input
- CVE-2025-20221 (CVSS 5.3) – Allows unauthenticated attackers to bypass Layer 3 and Layer 4 traffic filters by sending crafted packets to affected IOS XE SD-WAN devices
- CVE-2025-20147 (CVSS 6.5) – Cross-site scripting in Catalyst SD-WAN Manager (PoC available)
- CVE-2025-20137 (CVSS 4.7) – ACL bypass due to unsupported configuration; no patch planned

Aspire Protects

- **Patch –** Prioritize patching for CVE-2025-32433 and CVE-2025-20188.
- Audit device configurations to see if the vulnerable AP download feature is enabled.
- Disable vulnerable features if patching is delayed.
- Stay alert for PoC-based activity targeting exposed systems

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit vulnerable SSH services (CVE-2025-32433) or the Out-of-Band AP image download interface (CVE-2025-20188) to gain a foothold on exposed systems.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute arbitrary commands on the device after exploiting either vulnerability.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – In the case of CVE-2025-20188, successful exploitation grants root-level command execution.

Persistence

- Modify System Image [T1601.001] – Uploaded files via CVE-2025-20188 could allow attackers to maintain access or embed malicious code.

Defense Evasion

- Valid Accounts [T1078] – While these flaws don't require credentials, attackers could use initial access to create accounts or install SSH keys for future use.

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

Some environments are more exposed than others, depending on the Cisco products in use. Wireless controllers, orchestration tools, and SSH-based access points are common across the kinds of networks these vulnerabilities hit hardest.

- Healthcare
- Education
- Retail
- Finance
- Manufacturing
- Government
- Legal Services

Aspire 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 IOS XE Wireless Controller Software Arbitrary File Upload Vulnerability

Multiple Cisco Products Unauthenticated Remote Code Execution in Erlang/OTP SSH Server: April 2025