Multiple Cisco IOS XE Vulnerabilities and Actively Exploited SD-WAN Flaws Impact Network Infrastructure

TL;DR

Cisco released multiple patches for vulnerabilities across IOS XE, wireless controllers, switching platforms, and SD-WAN products. The vulnerabilities include CVE-2026-20122 (CVSS 7.1) and CVE-2026-20128 (CVSS 7.5), which are being actively exploited, along with CVE-2026-20129 (CVSS 9.8) that allows unauthenticated access to SD-WAN Manager.

Successful exploitation could lead to device crashes, network outages, unauthorized access, or full control of management systems.

Overview

There are multiple Cisco vulnerabilities impacting IOS XE Software, Catalyst switches, wireless controllers, and SD-WAN environments.

Cisco IOS XE Vulnerabilities Impact Switches, Controllers, and Management Interfaces

- CVE-2026-20104 (CVSS 6.1) – This vulnerability affects the boot process on certain Catalyst and rugged switches. An attacker with physical access or high privileges can bypass secure boot protections and run unsigned code during startup. This breaks the chain of trust and allows persistent control of the device.
- CVE-2026-20004 (CVSS 7.4) – A flaw in the TLS implementation allows an attacker on the same network to repeatedly consume device memory. Over time, this forces the device to reload and disrupt normal operations. It can be triggered through repeated authentication attempts or manipulated TLS sessions.
- CVE-2026-20086 (CVSS 8.6**)** – This vulnerability impacts wireless controllers handling CAPWAP traffic. A remote attacker can send malformed packets that cause the controller to crash and reload. This can knock wireless networks offline across an organization.
- CVE-2026-20125 **(**CVSS 7.7) – An issue in the HTTP server allows an authenticated user to send crafted requests that trigger a watchdog timeout. This causes the device to reload unexpectedly. Repeated use could lead to sustained service disruption.
- CVE-2026-20084 (CVSS 8.6) – This vulnerability affects DHCP snooping on Catalyst 9000 switches. An attacker can send BOOTP traffic that leaks across

VLANs and drives CPU usage up. The device can become unresponsive and stop forwarding traffic.

- CVE-2026-20108 (CVSS 5.4) – A cross-site scripting issue in SD-WAN Manager allows an attacker to trick a user into clicking a crafted link. This can lead to script execution within the management interface. Session data or user activity could be exposed.

- CVE-2026-20083 **(**CVSS 6.5) – The SCP server feature can be abused by a low-privileged user issuing a crafted command over SSH. This causes the device to reload and interrupts normal operations. It's an internal risk where access already exists.

- CVE-2026-20112 (CVSS 4.8) – A stored XSS vulnerability in the IOx environment allows an authenticated admin to inject malicious scripts. These scripts execute when other users access the interface. This can lead to session hijacking or unauthorized actions.

- CVE-2026-20113 (CVSS 5.3) – This issue allows CRLF injection in IOx logs. An attacker can manipulate or insert log entries to hide activity. This makes detection and investigation more difficult.

- CVE-2026-20115 (CVSS 6.1) – A vulnerability in the Meraki secure channel allows sensitive configuration data to be exposed. An attacker performing an on-path attack can view device information in transit. This could reveal network details useful for follow-on activity.

- CVE-2026-20110 (CVSS 6.5) – A privilege issue in the CLI allows a low-privileged user to trigger maintenance mode. This shuts down interfaces and interrupts traffic flow. An attacker could use this to disrupt business operations.

- CVE-2026-20114 (CVSS 5.4**)** – This vulnerability allows a Lobby Ambassador user to gain additional access through the API. A crafted request can lead to unauthorized account creation. This expands access to management functions that should be restricted.

Cisco Catalyst SD-WAN Vulnerabilities

- CVE-2026-20129 (CVSS 9.8) – An authentication bypass allows an unauthenticated attacker to access SD-WAN Manager as a privileged user. This

gives direct control over the system without valid credentials. From there, commands can be executed at a high privilege level.

- CVE-2026-20126 (CVSS 7.8) – A flaw in the API allows a low-privileged user to escalate privileges to root. This provides full control over the underlying operating system. An attacker could alter configurations or introduce malicious changes.

- CVE-2026-20133 (CVSS 7.5**)** – This vulnerability allows unauthorized access to sensitive system data. An attacker can retrieve files or system information through exposed API paths. This data can support further compromise.

- CVE-2026-20122 (CVSS 7.1) – This vulnerability allows an authenticated user to overwrite files on the system. Attackers can upload malicious files and replace existing ones. Cisco confirmed **active exploitation**.

- CVE-2026-20128 (CVSS 7.5**)** – A credential exposure issue allows attackers to retrieve sensitive authentication data. This can be used to access additional systems or services. Cisco also confirmed **active exploitation** of this vulnerability.

Aspire Protects

- **Patch** - Upgrade affected Cisco IOS XE and SD-WAN systems immediately. See Cisco's advisories for more information.
- Prioritize SD-WAN Manager patches due to active exploitation.
- Restrict access to management interfaces and APIs.
- Monitor logs for unusual activity, reloads, or API requests.
- Disable unused services such as HTTP, SCP, or IOx where possible.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may send crafted requests to exposed services such as SD-WAN Manager APIs, HTTP interfaces, or CAPWAP services to gain access or trigger exploitation (CVE-2026-20129, CVE-2026-20125, CVE-2026-20086).

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit weaknesses in APIs or access controls to elevate privileges or gain administrative access (CVE-2026-20126, CVE-2026-20114).

Execution

- User Execution [T1204] – The attacker may rely on a user interacting with malicious links or content to trigger script execution within management interfaces (CVE-2026-20108, CVE-2026-20112).

Defense Evasion

- Modify System Image [T1601] – The attacker may bypass secure boot protections to load unauthorized or modified system images during device startup (CVE-2026-20104).

Credential Access

- Credentials in Files [T1552] – The attacker may access sensitive credentials or configuration data exposed through vulnerable components or insecure communication channels (CVE-2026-20128, CVE-2026-20115).

Impact

- Endpoint Denial of Service [T1499] – The attacker may force devices to reload or become unavailable by exploiting memory exhaustion, malformed packet handling, or maintenance mode abuse (CVE-2026-20004, CVE-2026-20086, CVE-2026-20125, CVE-2026-20083, CVE-2026-20110, CVE-2026-20084).

- Data Manipulation [T1565] – The attacker may overwrite or modify files on the system to alter system behavior or gain further access (CVE-2026-20122).

IoCs

CVE-2026-20128 – Information Disclosure (SD-WAN Manager)

File Paths

- /var/log/nms/containers/service-proxy/serviceproxy-access.log
- /reports/data/opt/data/containers/config/data-collection-agent/.dca

Network Artifacts (HTTP Requests)

- GET /reports/data/opt/data/containers/config/data-collection-agent/.dca

User Agent

- python-requests/2.x

CVE-2026-20122 – Arbitrary File Overwrite (SD-WAN Manager)

File Paths

- /var/log/nms/containers/service-proxy/serviceproxy-access.log
- /var/log/nms/vmanage-server.log

- /cmd.gz/cmd.jsp

Network Artifacts (HTTP Requests)

- POST /dataservice/smartLicensing/uploadAck
- POST /cmd.gz/cmd.jsp

Indicators of Malicious Behavior

- Directory traversal patterns:
  - ../../../../../../
- File write activity to unexpected system paths

Targeted Industries

These vulnerabilities impact any organization using Cisco network infrastructure.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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 Software for Cisco Catalyst and Rugged Series Switches Secure Boot Bypass Vulnerability

Cisco IOS XE Software TLS Memory Exhaustion Denial of Service Vulnerability

Cisco IOS XE Wireless Controller Software for the Catalyst CW9800 Family CAPWAP Denial of Service Vulnerability

Cisco IOS Software and IOS XE Software Release 3E HTTP Server Denial of Service Vulnerability

Cisco IOS XE Software for Catalyst 9000 Series Switches DHCP Snooping Denial of Service Vulnerability

Cisco Catalyst SD-WAN Manager Cross-Site Scripting Vulnerability

Cisco IOS XE Software Secure Copy Protocol Server Denial of Service Vulnerability

Cisco IOx Application Hosting Environment Stored Cross-Site Scripting Vulnerability

Cisco IOx Application Hosting Environment Carriage Return Line Feed Injection Vulnerability

Cisco IOS XE Software Secure Channel for Meraki Information Disclosure Vulnerability

Cisco IOS XE Software Denial of Service Vulnerability

Cisco IOS XE Software Lobby Ambassador Privilege Escalation Vulnerability