Critical Cisco IOS XE Vulnerability Could Allow Unauthenticated Command Injection

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A critical vulnerability (CVE-2026-20272, CVSS 9.8) in Cisco IOS XE Software could allow an unauthenticated remote attacker to inject commands into an affected device. Cisco has released fixed software and confirmed there are no workarounds.

Overview

There is a critical vulnerability (CVE-2026-20272, CVSS 9.8) in Cisco IOS XE Software, which runs on routers and switches that keep users, offices and business systems connected. If an attacker compromises one of these devices, they could run unauthorized commands or change network behavior, potentially interrupting access to applications and other business services.

An attacker can reach the vulnerability remotely without credentials or user interaction. Cisco rates the attack complexity as low, which makes the flaw easier to exploit, although the company has not released technical details showing the exact attack method.

Affected Products

CVE-2026-20272 affects Cisco IOS XE Software running in autonomous or controller mode, regardless of device configuration.

- Cisco IOS XE 17.9 before 17.9.10
- Cisco IOS XE 17.12 before 17.12.8
- Cisco IOS XE 17.15 before 17.15.6
- Cisco IOS XE 17.18 before 17.18.4/17.18.4a
- Cisco IOS XE 26.1 before 26.1.2

Cisco found the vulnerability during internal testing and has not identified public exploit code or active attacks.

Aspire Protects

- Identify Cisco devices running IOS XE 17.9, 17.12, 17.15, 17.18 or 26.1 and confirm the installed release. See Cisco's advisory for more information.
- Upgrade affected devices to 17.9.10, 17.12.8, 17.15.6, 17.18.4, 17.18.4a or 26.1.2, based on the software branch in use.

- Use the Cisco Software Checker linked in the advisory to confirm whether a specific release is affected and identify the correct upgrade.
- Do not rely on configuration changes as a temporary fix. Cisco states that affected releases are vulnerable in autonomous and controller mode regardless of configuration, and no workarounds are available.

TTPs to Watch

Cisco has not released enough technical information about CVE-2026-20272 to map the vulnerability to a specific MITRE ATT&CK technique.

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 vulnerability can affect any organization using Cisco IOS XE devices to support its network, including:

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

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 Security Hardening Release: August 2026