Cisco IOS and IOS XE SNMP Zero-Day Exploited in the Wild

TL;DR

A new Cisco IOS and IOS XE vulnerability (CVE-2025-20352, CVSS 7.7) in the SNMP subsystem is being actively exploited. Attackers with SNMP credentials can cause denial-of-service or execute code as root, granting full device control.

No workarounds exist but Cisco has released fixes.

Overview

This week, Cisco released an advisory for CVE-2025-20352 (CVSS 7.7), a stack overflow vulnerability in the SNMP subsystem of IOS and IOS XE software. Authenticated, remote attackers can exploit the vulnerability by sending crafted SNMP packets over IPv4 or IPv6.

Affected Products

- Cisco IOS with SNMP enabled
- Cisco IOS XE with SNMP enabled
- Meraki MS390 running Meraki CS 17 and earlier
- Cisco Catalyst 9300 running Meraki CS 17 and earlier

Not Affected

- Cisco IOS XR
- Cisco NX-OS

Attackers with read-only SNMPv2c strings or SNMPv3 user credentials can cause denial-of-service, while those with administrative or privilege 15 (highest privilege level) credentials can execute code as root on IOS XE. Cisco confirmed exploitation in the wild after stolen administrator credentials were used. Successful exploitation allows attackers to either force device reloads or gain full system control, depending on their privilege level.

Aspire Protects

- **Patch** - Apply Cisco's fixed IOS and IOS XE software releases. Use Cisco Software Checker to identify the correct version.
- Limit SNMP to trusted users only

- Configure SNMP views to exclude vulnerable OIDs. Note this may disrupt device management.
- Rotate SNMP community strings and administrator credentials; monitor for unusual access.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit exposed SNMP services with crafted packets.

Execution

- Exploitation for Client Execution [T1203] – High-privileged attackers may execute arbitrary code as root on IOS XE.

Impact

- Service Stop [T1489] – Low-privileged attackers may cause devices to reload, resulting in denial-of-service.

IoCs

Targeted Industries

This vulnerability impacts any organization running Cisco IOS or IOS XE with SNMP enabled:

- 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 and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability