Old SNMP Flaws in Cisco IOS and IOS XE Still Being Exploited

TL;DR

Three old SNMP flaws (CVE-2017-6736, CVE-2017-6737, and CVE-2017-6738) continue to be exploited in the wild. CISA added CVE-2017-6736 and CVE-2017-6737 to its Known Exploited Vulnerabilities catalog back in 2022, due to widespread abuse.

These vulnerabilities affect Cisco IOS and IOS XE software with SNMP enabled and allow remote code execution or forced reboot.

Overview

Three old Cisco vulnerabilities (CVE-2017-6736, CVE-2017-6737, and CVE-2017-6738, CVSS 8.8) are making their rounds again. These bugs date back to 2017, yet they're still relevant today because many Cisco devices remain unpatched or are running outdated SNMP configurations. The flaws are tied to a buffer overflow issue in the SNMP subsystem. Attackers can send a specially crafted SNMP packet to a targeted device and either crash it or gain remote control.

Affected Products

- Cisco IOS (12.0 - 12.4, 15.0–15.6)
- Cisco IOS XE (2.2–3.17)
- Devices with SNMP enabled and MIBs such as:
    - *ADSL-LINE-MIB, ALPS-MIB, CISCO-BSTUN-MIB, CISCO-VOICE-DNIS-MIB*, and others

There are two ways attackers can exploit the vulnerability:

- For SNMP v2c or earlier, the attacker needs the read-only community string.
- For SNMP v3, valid credentials are required.

Cisco confirmed exploitation of all three CVEs stem from the same issue and noted that these attacks require the malicious traffic to be directed at the device (no broadcast-style abuse). SNMP must be enabled, and vulnerable MIBs must be active, which is the default in many cases. CISA added CVE-2017-6736 and CVE-2017-6737 to the Known Exploited Vulnerabilities (KEV) catalog in 2022 due to exploitation. Aspire recommends patching immediately to help prevent compromise.

Aspire Protects

- **Patch** – Aspire recommends patching immediately. Please see Cisco's advisory for patch guidance.
- Disable vulnerable MIBs using `snmp-server view` settings.
- Rotate community strings regularly. Avoid weak or default strings.
- Restrict SNMP, only allow from trusted IPs.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] - The attacker targets publicly reachable SNMP services with valid credentials.

Execution

- Exploitation for Client Execution [T1203] - Buffer overflow is triggered via a crafted SNMP packet.

Impact

- System Reboot [T1529] - Exploitation may crash the device and trigger an unexpected reboot.

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

These vulnerabilities affect a wide range of industries that rely on Cisco networking gear and SNMP-based monitoring,

- Finance
- Education
- Government
- Transportation
- Telecommunications
- Energy

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

Known Exploited Vulnerabilities Catalog | CISA

CVE Record: CVE-2017-6737

CVE Record: CVE-2017-6736

NVD - cve-2017-6738

SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software