CVE-2017-6743

Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability

CISA KEV since Mar 3, 2022 | Actively exploited

The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS and IOS XE Software contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100 Urgent priority	8.8 High · NVD	0.109 95.9th percentile · FIRST	Mar 24, 2022 KEV since 2022 · listed over a year

Signals behind the score

counted in the score | not counted — evidence for 6 of 8 signals

✓ CISA KEV	Listed in the catalog	− Vendor exploitation	Confirmed exploitation in the wild
− Ransomware	No known ransomware campaign association	− KEV recency	On the CISA KEV catalog for over two years
✓ EPSS	0.109 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 8.8	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle — Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
Basis: CISA KEV required action

The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP - Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. A successful exploit could allow the attacker to execute arbitrary code and obtain full control of the affected system or cause the affected system to reload. Customers are advised to apply the workaround as contained in the Workarounds section below. Fixed software information is available via the Cisco IOS Software Checker. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. There are workarounds that address these vulnerabilities.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	⩾ 12.0 ⩽ 12.4 ⩾ 15.0 ⩽ 15.6	after 12.4 · after 15.6	NVD
ios xe	⩾ 2.2.0 ⩽ 3.17	after 3.17	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-6g39-9vj5-c7xv	Additional guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp
NVD	nvd.nist.gov/vuln/detail/CVE-2017-6743	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-15797	Current data	evulnable.com/vulnerability-management/cve/CVE-2017-6743

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.