

CVE-2017-6737

Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

A vulnerability in the SNMP implementation of could allow an authenticated, remote attacker to cause a reload of the affected system or to remotely execute code. An attacker could exploit this vulnerability by sending a crafted SNMP packet to the affected device. The vulnerability is due to a buffer overflow in the affected code area. The vulnerability affects all versions of SNMP (versions 1, 2c, and 3).

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.452 98.8th percentile · FIRST	CISA DEADLINE 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	0.452 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 attacker must know the SNMP read only community string (SNMP version 2c or earlier) or the user credentials (SNMPv3). An exploit could allow the attacker to execute arbitrary code and obtain full control of the system or to cause a reload of the affected system. Only traffic directed to the affected system can be used to exploit this vulnerability.

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 ≤ 3.17.0	after 3.17.0	NVD

Sources

Vendor guidance github.com/advisories/GHSA-f29v-pr27-8f5j

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

NVD nvd.nist.gov/vuln/detail/CVE-2017-6737

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-15791

Current data evulnable.com/vulnerability-management/cve/CVE-2017-6737

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