

CVE-2017-6744

Cisco IOS 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 75/100 Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.073 94.3rd 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	0.073 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

ios	12.2\ (33\)sxi	no fixed version listed	NVD
	12.2\ (33\)sxi1		
	12.2\ (50\)se		
	12.2\ (50\)se1		
	12.2\ (50\)se2		
	12.2\ (50\)se3		
	12.2\ (50\)se4		
	12.2\ (50\)se5		
	12.2\ (50\)sg		
	12.2\ (50\)sg1		
	12.2\ (50\)sg2		
	12.2\ (50\)sg3		
	12.2\ (50\)sg4		
	12.2\ (50\)sg5		
	12.2\ (50\)sg6		
	12.2\ (50\)sg7		
	12.2\ (50\)sg8		
	12.2\ (50\)sq		
	12.2\ (50\)sq1		
	12.2\ (50\)sq2		
	12.2\ (50\)sq3		
	12.2\ (50\)sq4		
	12.2\ (50\)sq5		
	12.2\ (50\)sq6		
	12.2\ (50\)sq7		
	12.2\ (52\)ex		
	12.2\ (52\)ex1		
	12.2\ (52\)ey		
	12.2\ (52\)ey1		
	12.2\ (52\)ey1b		
	12.2\ (52\)ey1c		
	12.2\ (52\)ey2		
	12.2\ (52\)ey2a		
	12.2\ (52\)ey3		
	12.2\ (52\)ey3a		
	12.2\ (52\)ey4		
	12.2\ (52\)se		
	12.2\ (52\)se1		
	12.2\ (52\)sg		
	12.2\ (52\)xo		
	12.2\ (53\)ex		
	12.2\ (53\)ey		
	12.2\ (53\)ez		
	12.2\ (53\)se		
	12.2\ (53\)se1		
	12.2\ (53\)se2		
	12.2\ (53\)sg		
	12.2\ (53\)sg1		
	12.2\ (53\)sg2		
	12.2\ (53\)sg3		
	12.2\ (53\)sg4		
	12.2\ (53\)sg5		
	12.2\ (53\)sg6		
	12.2\ (53\)sg7		
	12.2\ (53\)sg8		
	12.2\ (53\)sg9		
	12.2\ (53\)sg10		
	12.2\ (53\)sg11		
	12.2\ (54\)se		
	12.2\ (54\)sg		
	12.2\ (54\)sg1		
	12.2\ (54\)wo		
	12.2\ (54\)xo		

12.2\55\ex
12.2\55\ex1
12.2\55\ex2
12.2\55\ex3
12.2\55\ey
12.2\55\ez
12.2\55\se
12.2\55\se1
12.2\55\se2
12.2\55\se3
12.2\55\se4
12.2\55\se5
12.2\55\se6
12.2\55\se7
12.2\55\se8
12.2\55\se9
12.2\55\se10
12.2\55\se11
12.2\58\ex
12.2\58\ey
12.2\58\ey1
12.2\58\ey2
12.2\58\ez
12.2\58\se
12.2\58\se1
12.2\58\se2
12.2\60\ez
12.2\60\ez1
12.2\60\ez2
12.2\60\ez3
12.2\60\ez4
12.2\60\ez5
12.2\60\ez6
12.2\60\ez7
12.2\60\ez8
12.2\60\ez9
12.2\60\ez10
12.2\60\ez11
15.0\1\ex
15.0\1\ey
15.0\1\ey1
15.0\1\ey2
15.0\1\se
15.0\1\se1
15.0\1\se2
15.0\1\se3
15.0\1\xo
15.0\1\xo1
15.0\2\ea1
15.0\2\eb
15.0\2\ec
15.0\2\ed
15.0\2\ed1
15.0\2\eh
15.0\2\ej
15.0\2\ej1
15.0\2\ek
15.0\2\ek1
15.0\2\ex
15.0\2\ex1
15.0\2\ex2
15.0\2\ex3
15.0\2\ex4
15.0\2\ex5

15.0\2\ex8
15.0\2\ex10
15.0\2\ey
15.0\2\ey1
15.0\2\ey2
15.0\2\ey3
15.0\2\ez
15.0\2\se
15.0\2\se1
15.0\2\se2
15.0\2\se3
15.0\2\se4
15.0\2\se5
15.0\2\se6
15.0\2\se7
15.0\2\se9
15.0\2\se10
15.0\2\se10a
15.0\2\sg
15.0\2\sg1
15.0\2\sg2
15.0\2\sg3
15.0\2\sg4
15.0\2\sg5
15.0\2\sg6
15.0\2\sg7
15.0\2\sg8
15.0\2\sg9
15.0\2\sg10
15.0\2\sg11
15.0\2\sqd
15.0\2\sqd1
15.0\2\sqd2
15.0\2\sqd3
15.0\2\sqd5
15.0\2\sqd6
15.0\2\xo
15.0\2a\ex5
15.0\2a\se9
15.1\1\sg
15.1\1\sg1
15.1\1\sg2
15.1\2\sg
15.1\2\sg1
15.1\2\sg2
15.1\2\sg3
15.1\2\sg4
15.1\2\sg5
15.1\2\sg6
15.1\2\sg7
15.1\2\sg8
15.2\1\ey
15.2\1\ey1
15.2\1\ey2
15.2\1\ey3
15.2\1\ey
15.2\1\sy
15.2\1\sy0a
15.2\1\sy1
15.2\1\sy1a
15.2\1\sy2
15.2\1\sy3
15.2\1\sy4
15.2\2\ey

Generated Oct 22, 2026, 10:36 AM ET · Sources: NVD, CISA KEV, FIRST EPSS, GitHub Advisory Database (CC BY 4.0), ENISA EUVD

15.2\4m\e1
15.2\4m\e3
15.2\4p\e1
15.2\5\e
15.2\5\e1
15.2\5\e2
15.2\5\e2a
15.2\5\ea
15.2\5\ex
15.2\5a\e
15.2\5a\e1
15.2\5b\e
15.2\5c\e
15.3\1\sy
15.3\1\sy2
15.3\1\t
15.3\1\t1
15.3\1\t2
15.3\1\t3
15.3\1\t4
15.3\2\t
15.3\2\t1
15.3\2\t2
15.3\2\t3
15.3\2\t4
15.3\3\m
15.3\3\m1
15.3\3\m2
15.3\3\m3
15.3\3\m4
15.3\3\m5
15.3\3\m6
15.3\3\m7
15.3\3\m9
15.4\1\cg
15.4\1\cg1
15.4\1\sy
15.4\1\sy1
15.4\1\sy2
15.4\1\t
15.4\1\t1
15.4\1\t2
15.4\1\t3
15.4\1\t4
15.4\2\cg
15.4\2\t
15.4\2\t1
15.4\2\t2
15.4\2\t3
15.4\2\t4
15.4\3\m
15.4\3\m1
15.4\3\m2
15.4\3\m3
15.4\3\m4
15.4\3\m5
15.4\3\m6
15.4\3\m6a
15.4\3\m7
15.5\1\sy
15.5\1\t
15.5\1\t1
15.5\1\t2
15.5\1\t3

PACKAGE	AFFECTED	FIXED IN	SOURCE
	15.5\1\1\t4		
	15.5\2\1\t		
	15.5\2\2\t1		
	15.5\2\2\t2		
	15.5\2\2\t3		
	15.5\2\2\t4		
	15.5\3\1\m0a		
	15.5\3\1\m1		
	15.5\3\1\m2		
	15.5\3\1\m3		
	15.5\3\1\m4		
	15.5\3\1\m4a		
	15.5\3\1\m5		
	15.5\3\1\m6		
	15.6\1\1\t		
	15.6\1\1\t0a		
	15.6\1\1\t1		
	15.6\1\1\t2		
	15.6\2\1\t		
	15.6\2\1\t1		
	15.6\2\1\t2		
	15.6\3\1\m		
	15.6\3\1\m0a		
	15.6\3\1\m1		
	15.6\3\1\m1b		
	15.6\3\1\m2		
	15.6\3\1\m2a		
	15.6\3\1\m3		

Sources

Vendor guidance github.com/advisories/GHSA-7r2m-r994-47mm

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

NVD nvd.nist.gov/vuln/detail/CVE-2017-6744

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

ENISA EUVD euvsd.enisa.europa.eu/vulnerability/EUVD-2017-15798

Current data evulnable.com/vulnerability-management/cve/CVE-2017-6744

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