

CVE-2025-20352

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

CISA KEV since Sep 29, 2025

Actively exploited

A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software could allow the following: An authenticated, remote attacker with low privileges could cause a denial of service (DoS) condition on an affected device that is running Cisco IOS Software or Cisco IOS XE Software. To cause the DoS, the attacker must have the SNMPv2c or earlier read-only community string or valid SNMPv3 user credentials.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.7 High · NVD	EPSS 0.415 98.7th percentile · FIRST	CISA DEADLINE Oct 20, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.415 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

An authenticated, remote attacker with high privileges could execute code as the root user on an affected device that is running Cisco IOS XE Software. To execute code as the root user, the attacker must have the SNMPv1 or v2c read-only community string or valid SNMPv3 user credentials and administrative or privilege 15 credentials on the affected device. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks. This vulnerability is due to a stack overflow condition in the SNMP subsystem of the affected software. A successful exploit could allow a low-privileged attacker to cause the affected system to reload, resulting in a DoS condition, or allow a high-privileged attacker to execute arbitrary code as the root user and obtain full control of the affected system. Note: This vulnerability affects all versions of SNMP.



Affected and fixed versions



ios xe sd-wan	16.9.1	no fixed version listed	NVD
	16.9.2		
	16.9.3		
	16.9.4		
	16.10.1		
	16.10.2		
	16.10.3		
	16.10.3a		
	16.10.3b		
	16.10.4		
	16.10.5		
	16.10.6		
	16.11.1a		
	16.12.1b		
	16.12.1d		
	16.12.1e		
	16.12.2r		
	16.12.3		
	16.12.4		
	16.12.4a		
	16.12.5		



ios xe	3.5.0e	no fixed version listed	NVD
	3.5.0sq		
	3.5.1e		
	3.5.1sq		
	3.5.2e		
	3.5.2sq		
	3.5.3e		
	3.5.3sq		
	3.5.4sq		
	3.5.5sq		
	3.5.6sq		
	3.5.7sq		
	3.5.8sq		
	3.6.0e		
	3.6.1e		
	3.6.2ae		
	3.6.2e		
	3.6.3e		
	3.6.4e		
	3.6.5ae		
	3.6.5e		
	3.6.6e		
	3.6.7be		
	3.6.7e		
	3.6.8e		
	3.6.9e		
	3.6.10e		
	3.7.0e		
	3.7.1e		
	3.7.2e		
	3.7.3e		
	3.7.4e		
	3.7.5e		
	3.8.0e		
	3.8.1e		
	3.8.2e		
	3.8.3e		
	3.8.4e		
	3.8.5ae		
	3.8.5e		
	3.8.6e		
	3.8.7e		
	3.8.8e		
	3.8.9e		
	3.8.10e		
	3.9.0e		
	3.9.1e		
	3.9.2e		
	3.10.0ce		
	3.10.0e		
	3.10.1e		
	3.10.2e		
	3.10.3e		
	3.11.0e		
	3.11.1ae		
	3.11.1e		
	3.11.2e		
	3.11.3ae		
	3.11.3e		
	3.11.4e		
	3.11.5e		
	3.11.6e		
	3.11.7e		

3.11.8e
3.11.9e
3.11.10e
3.11.11e
3.11.12e
3.14.0s
3.14.1s
3.14.2s
3.14.3s
3.14.4s
3.15.0s
3.15.1cs
3.15.1s
3.15.2s
3.15.3s
3.15.4s
3.16.0cs
3.16.0s
3.16.1as
3.16.1s
3.16.2as
3.16.2bs
3.16.2s
3.16.3as
3.16.3s
3.16.4as
3.16.4bs
3.16.4ds
3.16.4s
3.16.5s
3.16.6bs
3.16.6s
3.16.7as
3.16.7bs
3.16.7s
3.16.8s
3.16.9s
3.16.10s
3.17.0s
3.17.1as
3.17.1s
3.17.2s
3.17.3s
3.17.4s
3.18.0as
3.18.0s
3.18.0sp
3.18.1asp
3.18.1bsp
3.18.1csp
3.18.1s
3.18.1sp
3.18.2asp
3.18.2s
3.18.2sp
3.18.3asp
3.18.3bsp
3.18.3s
3.18.3sp
3.18.4s
3.18.4sp
3.18.5sp
3.18.6sp
3.18.7sp

3.18.8asp
3.18.9sp
16.6.1
16.6.2
16.6.3
16.6.4
16.6.4a
16.6.5
16.6.5a
16.6.6
16.6.7
16.6.8
16.6.9
16.6.10
16.7.1
16.7.1a
16.7.1b
16.7.2
16.7.3
16.7.4
16.8.1
16.8.1a
16.8.1b
16.8.1c
16.8.1d
16.8.1e
16.8.1s
16.8.2
16.8.3
16.9.1
16.9.1a
16.9.1b
16.9.1s
16.9.2
16.9.3
16.9.3a
16.9.4
16.9.5
16.9.5f
16.9.6
16.9.7
16.9.8
16.10.1
16.10.1a
16.10.1b
16.10.1c
16.10.1d
16.10.1e
16.10.1f
16.10.1g
16.10.1s
16.10.2
16.10.3
16.11.1
16.11.1a
16.11.1b
16.11.1s
16.11.2
16.12.1
16.12.1a
16.12.1c
16.12.1s
16.12.1t
16.12.1w

16.12.1x
16.12.1y
16.12.1z1
16.12.1z2
16.12.2
16.12.2a
16.12.2s
16.12.3
16.12.3a
16.12.3s
16.12.4
16.12.4a
16.12.5
16.12.5a
16.12.5b
16.12.6
16.12.6a
16.12.7
16.12.8
16.12.9
16.12.10
16.12.10a
16.12.11
16.12.12
16.12.13
17.1.1
17.1.1a
17.1.1s
17.1.1t
17.1.3
17.2.1
17.2.1a
17.2.1r
17.2.1v
17.2.2
17.2.3
17.3.1
17.3.1a
17.3.1w
17.3.1x
17.3.1z
17.3.2
17.3.2a
17.3.3
17.3.4
17.3.4a
17.3.4b
17.3.4c
17.3.5
17.3.5a
17.3.5b
17.3.6
17.3.7
17.3.8
17.3.8a
17.4.1
17.4.1a
17.4.1b
17.4.2
17.4.2a
17.5.1
17.5.1a
17.6.1
17.6.1a

17.6.1w
17.6.1x
17.6.1y
17.6.1z
17.6.1z1
17.6.2
17.6.3
17.6.3a
17.6.4
17.6.5
17.6.5a
17.6.6
17.6.6a
17.6.7
17.6.8
17.6.8a
17.7.1
17.7.1a
17.7.1b
17.7.2
17.8.1
17.8.1a
17.9.1
17.9.1a
17.9.1w
17.9.1x
17.9.1x1
17.9.1y
17.9.1y1
17.9.2
17.9.2a
17.9.3
17.9.3a
17.9.4
17.9.4a
17.9.5
17.9.5a
17.9.5b
17.9.5e
17.9.5f
17.9.6
17.9.6a
17.9.7
17.9.7a
17.9.7b
17.10.1
17.10.1a
17.10.1b
17.11.1
17.11.1a
17.12.1
17.12.1a
17.12.1w
17.12.1x
17.12.1y
17.12.1z
17.12.1z1
17.12.1z2
17.12.1z3
17.12.1z4
17.12.2
17.12.2a
17.12.3
17.12.3a

PACKAGE	AFFECTED	FIXED IN	SOURCE
	17.12.4		
	17.12.4a		
	17.12.4b		
	17.12.5		
	17.12.5a		
	17.12.5b		
	17.12.5c		
	17.13.1		
	17.13.1a		
	17.14.1		
	17.14.1a		
	17.15.1		
	17.15.1a		
	17.15.1b		
	17.15.1w		
	17.15.1x		
	17.15.1y		
	17.15.1z		
	17.15.2		
	17.15.2a		
	17.15.2b		
	17.15.2c		
	17.15.3		
	17.15.3a		
	17.15.3b		
	17.15.4		
	17.16.1		
	17.16.1a		
	17.17.1		
	17.18.1		



ios	12.2\33\)\sxi	no fixed version listed	NVD
	12.2\33\)\sxi1		
	12.2\33\)\sxi2		
	12.2\33\)\sxi2a		
	12.2\33\)\sxi3		
	12.2\33\)\sxi4		
	12.2\33\)\sxi4a		
	12.2\33\)\sxi5		
	12.2\33\)\sxi6		
	12.2\33\)\sxi7		
	12.2\33\)\sxi8		
	12.2\33\)\sxi8a		
	12.2\33\)\sxi9		
	12.2\33\)\sxi10		
	12.2\33\)\sxi11		
	12.2\33\)\sxi12		
	12.2\33\)\sxi13		
	12.2\33\)\sxi14		
	12.2\33\)\sxj		
	12.2\33\)\sxj1		
	12.2\33\)\sxj2		
	12.2\33\)\sxj3		
	12.2\33\)\sxj4		
	12.2\33\)\sxj5		
	12.2\33\)\sxj6		
	12.2\33\)\sxj7		
	12.2\33\)\sxj8		
	12.2\33\)\sxj9		
	12.2\33\)\sxj10		
	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\53\)\ez		
	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\55\)\se12		
	12.2\55\)\se13		
	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
12.2\60\ez12
12.2\60\ez13
12.2\60\ez14
12.2\60\ez15
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\sy
15.0\1\sy1
15.0\1\sy2
15.0\1\sy3
15.0\1\sy4
15.0\1\sy5
15.0\1\sy6
15.0\1\sy7
15.0\1\sy7a
15.0\1\sy8
15.0\1\sy9
15.0\1\sy10
15.0\2\ea
15.0\2\ea1
15.0\2\ej
15.0\2\ej1
15.0\2\ek
15.0\2\ek1
15.0\2\ey
15.0\2\ey1
15.0\2\ey2
15.0\2\ey3
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\se8
15.0\2\se9
15.0\2\se10
15.0\2\se10a
15.0\2\se11
15.0\2\se12
15.0\2\se13
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\sqd4
15.0\2\sqd5
15.0\2\sqd6
15.0\2\sqd7
15.0\2\sqd8
15.1\1\sg
15.1\1\sg1
15.1\1\sg2
15.1\1\sy
15.1\1\sy1
15.1\1\sy2
15.1\1\sy3
15.1\1\sy4
15.1\1\sy5
15.1\1\sy6
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
15.1\2\sy
15.1\2\sy1
15.1\2\sy2
15.1\2\sy3
15.1\2\sy4
15.1\2\sy4a
15.1\2\sy5
15.1\2\sy6
15.1\2\sy7
15.1\2\sy8
15.1\2\sy9
15.1\2\sy10
15.1\2\sy11
15.1\2\sy12
15.1\2\sy13
15.1\2\sy14
15.1\2\sy15
15.1\2\sy16
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\1\sy5
15.2\1\sy6
15.2\1\sy7
15.2\1\sy8

Generated Oct 22, 2026, 4:41 PM ET · Sources: NVD, CISA KEV, FIRST EPSS, GitHub Advisory Database (CC BY 4.0), ENISA EUVD



15.2\4\ec2
15.2\4\gc
15.2\4\gc1
15.2\4\gc2
15.2\4\gc3
15.2\4\jb
15.2\4\jb1
15.2\4\jb2
15.2\4\jb3
15.2\4\jb3a
15.2\4\jb3b
15.2\4\jb3h
15.2\4\jb4
15.2\4\jb5
15.2\4\jb6
15.2\4\jn
15.2\4\m
15.2\4\m1
15.2\4\m2
15.2\4\m3
15.2\4\m4
15.2\4\m5
15.2\4\m6
15.2\4\m6a
15.2\4\m7
15.2\4\m8
15.2\4\m9
15.2\4\m10
15.2\4\m11
15.2\5\e
15.2\5\e1
15.2\5\e2
15.2\5\e2c
15.2\5\ea
15.2\5\ex
15.2\5a\e
15.2\5a\e1
15.2\5b\e
15.2\5c\e
15.2\6\e
15.2\6\e0a
15.2\6\e0c
15.2\6\e1
15.2\6\e2
15.2\6\e2a
15.2\6\e2b
15.2\6\e3
15.2\7\e
15.2\7\e0a
15.2\7\e0b
15.2\7\e0s
15.2\7\e1
15.2\7\e1a
15.2\7\e2
15.2\7\e2a
15.2\7\e3
15.2\7\e3k
15.2\7\e4
15.2\7\e5
15.2\7\e6
15.2\7\e7
15.2\7\e8
15.2\7\e9
15.2\7\e10



15.2\ (7\)e11
15.2\ (7\)e12
15.2\ (7a\)e0b
15.2\ (7b\)e0b
15.2\ (8\)e
15.2\ (8\)e1
15.2\ (8\)e2
15.2\ (8\)e3
15.2\ (8\)e4
15.2\ (8\)e5
15.2\ (8\)e6
15.2\ (8\)e7
15.3\ (1\)sy
15.3\ (1\)sy1
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\)ja1
15.3\ (3\)ja1m
15.3\ (3\)ja4
15.3\ (3\)ja5
15.3\ (3\)ja6
15.3\ (3\)ja7
15.3\ (3\)ja8
15.3\ (3\)ja10
15.3\ (3\)ja11
15.3\ (3\)ja12
15.3\ (3\)jaa
15.3\ (3\)jaa11
15.3\ (3\)jaa12
15.3\ (3\)jab
15.3\ (3\)jax
15.3\ (3\)jax1
15.3\ (3\)jax2
15.3\ (3\)jb
15.3\ (3\)jbb
15.3\ (3\)jbb1
15.3\ (3\)jbb2
15.3\ (3\)jbb4
15.3\ (3\)jbb5
15.3\ (3\)jbb6
15.3\ (3\)jbb6a
15.3\ (3\)jbb8
15.3\ (3\)jc
15.3\ (3\)jc1
15.3\ (3\)jc2
15.3\ (3\)jc3
15.3\ (3\)jc4
15.3\ (3\)jc5
15.3\ (3\)jc6
15.3\ (3\)jc8
15.3\ (3\)jc9
15.3\ (3\)jc14
15.3\ (3\)jca7
15.3\ (3\)jca8
15.3\ (3\)jca9



15.3\3\jd
15.3\3\jd2
15.3\3\jd3
15.3\3\jd4
15.3\3\jd5
15.3\3\jd6
15.3\3\jd7
15.3\3\jd8
15.3\3\jd9
15.3\3\jd11
15.3\3\jd13
15.3\3\jd14
15.3\3\jd16
15.3\3\jd17
15.3\3\jda7
15.3\3\jda8
15.3\3\jda9
15.3\3\jda11
15.3\3\jda13
15.3\3\jda14
15.3\3\jda16
15.3\3\jda17
15.3\3\je
15.3\3\jf
15.3\3\jf1
15.3\3\jf2
15.3\3\jf4
15.3\3\jf5
15.3\3\jf6
15.3\3\jf7
15.3\3\jf8
15.3\3\jf9
15.3\3\jf10
15.3\3\jf11
15.3\3\jf12
15.3\3\jf12i
15.3\3\jf14
15.3\3\jf14i
15.3\3\jf15
15.3\3\jg
15.3\3\jg1
15.3\3\jh
15.3\3\jh1
15.3\3\ji1
15.3\3\ji3
15.3\3\ji4
15.3\3\ji5
15.3\3\ji6
15.3\3\jj
15.3\3\jj1
15.3\3\jk
15.3\3\jk1
15.3\3\jk1t
15.3\3\jk2
15.3\3\jk2a
15.3\3\jk3
15.3\3\jk4
15.3\3\jk5
15.3\3\jk6
15.3\3\jk7
15.3\3\jk8
15.3\3\jk8a
15.3\3\jk8b
15.3\3\jk9



15.3\3\jk10
15.3\3\jk11
15.3\3\jn3
15.3\3\jn4
15.3\3\jn7
15.3\3\jn8
15.3\3\jn9
15.3\3\jnb
15.3\3\jnb1
15.3\3\jnb2
15.3\3\jnb3
15.3\3\jnb4
15.3\3\jnb5
15.3\3\jnb6
15.3\3\jnc
15.3\3\jnc1
15.3\3\jnc4
15.3\3\jnd
15.3\3\jnd1
15.3\3\jnd2
15.3\3\jnd3
15.3\3\jnp
15.3\3\jnp1
15.3\3\jnp3
15.3\3\jpb
15.3\3\jpb1
15.3\3\jpc
15.3\3\jpc1
15.3\3\jpc2
15.3\3\jpc3
15.3\3\jpc5
15.3\3\jpd
15.3\3\jpi1
15.3\3\jpi1t
15.3\3\jpi4
15.3\3\jpi5
15.3\3\jpi6a
15.3\3\jpi7
15.3\3\jpi8a
15.3\3\jpi9
15.3\3\jpi10
15.3\3\jpi2
15.3\3\jpi2t
15.3\3\jpi3
15.3\3\jpi3a
15.3\3\jpi4
15.3\3\jpi5
15.3\3\jpi6
15.3\3\jpi7
15.3\3\jpi7c
15.3\3\jpi8a
15.3\3\jpi9
15.3\3\jpi10
15.3\3\jpi11
15.3\3\jpk
15.3\3\jpk1
15.3\3\jpk2
15.3\3\jpk3
15.3\3\jpk4
15.3\3\jpk5
15.3\3\jpk6
15.3\3\jpk7
15.3\3\jpk8
15.3\3\jpk9



15.3\3\jpl
15.3\3\jpm
15.3\3\jpn
15.3\3\jpn1
15.3\3\jpn2
15.3\3\jpn3
15.3\3\jpn4
15.3\3\jpn5
15.3\3\jpn6
15.3\3\jpo
15.3\3\jpp
15.3\3\jprq
15.3\3\jprq1
15.3\3\jprq2
15.3\3\jprq3
15.3\3\jprq4
15.3\3\jprq5
15.3\3\jpr
15.3\3\jps
15.3\3\jpt
15.3\3\jpt1
15.3\3\jpt2
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\m8
15.3\3\m8a
15.3\3\m9
15.3\3\m10
15.4\1\cg
15.4\1\cg1
15.4\1\sy
15.4\1\sy1
15.4\1\sy2
15.4\1\sy3
15.4\1\sy4
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
15.5\1\s
15.5\1\s1
15.5\1\s2
15.5\1\s3
15.5\1\s4
15.5\1\sy
15.5\1\sy1
15.5\1\sy2
15.5\1\sy3
15.5\1\sy4
15.5\1\sy5
15.5\1\sy6



15.5\1\sy7
15.5\1\sy8
15.5\1\sy9
15.5\1\sy10
15.5\1\sy11
15.5\1\sy12
15.5\1\sy13
15.5\1\sy14
15.5\1\sy15
15.5\1\t
15.5\1\t1
15.5\1\t2
15.5\1\t3
15.5\1\t4
15.5\2\s
15.5\2\s1
15.5\2\s2
15.5\2\s3
15.5\2\s4
15.5\2\t
15.5\2\t1
15.5\2\t2
15.5\2\t3
15.5\2\t4
15.5\3\m
15.5\3\m0a
15.5\3\m1
15.5\3\m2
15.5\3\m3
15.5\3\m4
15.5\3\m4a
15.5\3\m5
15.5\3\m6
15.5\3\m6a
15.5\3\m7
15.5\3\m8
15.5\3\m9
15.5\3\m10
15.5\3\s
15.5\3\s0a
15.5\3\s1
15.5\3\s1a
15.5\3\s2
15.5\3\s3
15.5\3\s4
15.5\3\s5
15.5\3\s6
15.5\3\s6a
15.5\3\s6b
15.5\3\s7
15.5\3\s8
15.5\3\s9
15.5\3\s9a
15.5\3\s10
15.5\3\sn
15.6\1\s
15.6\1\s1
15.6\1\s2
15.6\1\s3
15.6\1\s4
15.6\1\t
15.6\1\t0a
15.6\1\t1
15.6\1\t2



15.6\1\t3
15.6\2\s
15.6\2\s1
15.6\2\s2
15.6\2\s3
15.6\2\s4
15.6\2\sn
15.6\2\sp
15.6\2\sp1
15.6\2\sp2
15.6\2\sp3
15.6\2\sp4
15.6\2\sp5
15.6\2\sp6
15.6\2\sp7
15.6\2\sp8
15.6\2\sp9
15.6\2\t
15.6\2\t1
15.6\2\t2
15.6\2\t3
15.6\3\m
15.6\3\m0a
15.6\3\m1
15.6\3\m1b
15.6\3\m2
15.6\3\m2a
15.6\3\m3
15.6\3\m3a
15.6\3\m4
15.6\3\m5
15.6\3\m6
15.6\3\m6a
15.6\3\m6b
15.6\3\m7
15.6\3\m8
15.6\3\m9
15.7\3\m
15.7\3\m0a
15.7\3\m1
15.7\3\m2
15.7\3\m3
15.7\3\m4
15.7\3\m4a
15.7\3\m4b
15.7\3\m5
15.7\3\m6
15.7\3\m7
15.7\3\m8
15.7\3\m9
15.8\3\m
15.8\3\m0a
15.8\3\m0b
15.8\3\m1
15.8\3\m1a
15.8\3\m2
15.8\3\m2a
15.8\3\m3
15.8\3\m3a
15.8\3\m3b
15.8\3\m4
15.8\3\m5
15.8\3\m6
15.8\3\m7



PACKAGE	AFFECTED	FIXED IN	SOURCE
	15.8\3\m8		
	15.8\3\m9		
	15.9\3\m		
	15.9\3\m0a		
	15.9\3\m1		
	15.9\3\m2		
	15.9\3\m2a		
	15.9\3\m3		
	15.9\3\m3a		
	15.9\3\m3b		
	15.9\3\m4		
	15.9\3\m4a		
	15.9\3\m5		
	15.9\3\m6		
	15.9\3\m6a		
	15.9\3\m6b		
	15.9\3\m7		
	15.9\3\m7a		
	15.9\3\m8		
	15.9\3\m8b		
	15.9\3\m9		
	15.9\3\m10		
	15.9\3\m11		

Sources

Vendor guidance github.com/advisories/GHSA-c924-mch4-p3p3

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

NVD nvd.nist.gov/vuln/detail/CVE-2025-20352

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-31023

Current data evulnable.com/vulnerability-management/cve/CVE-2025-20352

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