

CVE-2017-6663

Cisco IOS Software and Cisco IOS XE Software Denial-of-Service Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

A vulnerability in the Autonomic Networking feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause autonomic nodes of an affected system to reload, resulting in a denial of service (DoS) condition. More Information: CSCvd88936. Known Affected Releases: Denali-16.2.1 Denali-16.3.1.

EVRS 75/100 Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.021 81.7th 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	0.021 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ 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

Affected and fixed versions

ios	15.2\3\	e	no fixed version listed	NVD
	15.2\3\	e1		
	15.2\3\	e2		
	15.2\3\	e3		
	15.2\3\	e4		
	15.2\3\	e5		
	15.2\3a\	e		
	15.2\3a\	e1		
	15.2\3m\	e2		
	15.2\3m\	e3		
	15.2\3m\	e6		
	15.2\3m\	e8		
	15.2\4\	e		
	15.2\4\	e1		
	15.2\4\	e2		
	15.2\4\	e3		
	15.2\5\	e		
	15.2\5\	e1		
	15.2\5a\	e		
	15.2\5b\	e		
	15.3\3\	s		
	15.3\3\	s1		
	15.3\3\	s1a		
	15.3\3\	s2		
	15.3\3\	s3		
	15.3\3\	s4		
	15.3\3\	s5		
	15.3\3\	s6		
	15.3\3\	s7		
	15.3\3\	s8		
	15.3\3\	s8a		
	15.3\3\	s9		
	15.3\3\	s10		
	15.4\1\	s		
	15.4\1\	s1		
	15.4\1\	s2		
	15.4\1\	s3		
	15.4\1\	s4		
	15.4\2\	s		
	15.4\2\	s1		
	15.4\2\	s2		
	15.4\2\	s3		
	15.4\2\	s4		
	15.4\3\	s		
	15.4\3\	s1		
	15.4\3\	s2		
	15.4\3\	s3		
	15.4\3\	s4		
	15.4\3\	s5		
	15.4\3\	s5a		
	15.4\3\	s6		
	15.4\3\	s6a		
	15.4\3\	s6b		
	15.4\3\	s7		
	15.4\3\	s7a		
	15.4\3\	s8		
	15.5\1\	s		
	15.5\1\	s1		
	15.5\1\	s2		
	15.5\1\	s3		
	15.5\1\	s4		
	15.5\2\	s		
	15.5\2\	s1		



15.5\2\2)s2
15.5\2\2)s3
15.5\2\2)s4
15.5\3\3)s
15.5\3\3)s0a
15.5\3\3)s1
15.5\3\3)s1a
15.5\3\3)s2
15.5\3\3)s2a
15.5\3\3)s2b
15.5\3\3)s3
15.5\3\3)s3a
15.5\3\3)s4
15.5\3\3)s4a
15.5\3\3)s4b
15.5\3\3)s4d
15.5\3\3)s5
15.5\3\3)sn
15.6\1\1)s
15.6\1\1)s1
15.6\1\1)s1a
15.6\1\1)s2
15.6\1\1)s3
15.6\1\1)s4
15.6\1\1)t
15.6\1\1)t0a
15.6\1\1)t1
15.6\1\1)t2
15.6\2\2)s
15.6\2\2)s0a
15.6\2\2)s1
15.6\2\2)s2
15.6\2\2)s3
15.6\2\2)s4
15.6\2\2)sn
15.6\2\2)sp
15.6\2\2)sp1
15.6\2\2)sp1b
15.6\2\2)sp1c
15.6\2\2)sp2
15.6\2\2)sp2a
15.6\2\2)sp3
15.6\2\2)t
15.6\2\2)t1
15.6\2\2)t2
15.6\2\2)t3
15.6\3\3)m
15.6\3\3)m0a
15.6\3\3)m1
15.6\3\3)m1b
15.6\3\3)m2
15.6\3\3)m2a
15.6\3\3)m3
15.7\3\3)m

ios xe	3.7.0e	no fixed version listed	NVD
	3.7.1e		
	3.7.3e		
	3.8.0e		
	3.8.0ex		
	3.8.1e		
	3.8.2e		
	3.8.3e		
	3.9.0e		
	3.9.1e		
	3.10.4s		
	3.10.8as		
	3.10.8s		
	3.11.3s		
	3.11.4s		
	3.12.0as		
	3.12.0s		
	3.12.1s		
	3.12.2s		
	3.12.3s		
	3.12.4s		
	3.13.0s		
	3.13.1s		
	3.13.2as		
	3.13.2s		
	3.13.4s		
	3.13.5as		
	3.13.5s		
	3.13.6as		
	3.13.6s		
	3.13.7as		
	3.13.8s		
	3.14.0s		
	3.14.1s		
	3.14.2s		
	3.14.3s		
	3.14.4s		
	3.15.0s		
	3.15.1s		
	3.15.2s		
	3.15.3s		
	3.15.4s		
	3.16.0s		
	3.16.1as		
	3.16.2as		
	3.16.2s		
	3.16.3as		
	3.16.3s		
	3.16.4as		
	3.16.4ds		
	3.16.4s		
	3.16.6s		
	3.17.0s		
	3.17.1as		
	3.17.1s		
	3.17.3s		
	3.17.4s		
	3.18.0as		
	3.18.0s		
	3.18.0sp		
	3.18.1bsp		
	3.18.1s		
	3.18.1sp		



PACKAGE	AFFECTED	FIXED IN	SOURCE
	3.18.2asp		
	3.18.2s		
	3.18.2sp		
	3.18.3s		
	3.18.3sp		
	16.6.1		

Sources

Vendor guidance	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anidos	NVD	nvd.nist.gov/vuln/detail/CVE-2017-6663
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-15717
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-6663		

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