

CVE-2017-12231

Cisco IOS Software Network Address Translation Denial-of-Service Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

A vulnerability in the implementation of Network Address Translation (NAT) functionality in Cisco IOS 12.4 through 15.6 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to the improper translation of H.323 messages that use the Registration, Admission, and Status (RAS) protocol and are sent to an affected device via IPv4 packets.

EVRs

75_{/100}

Urgent priority

CVSS V3.1

7.5

High · NVD

EPSS

0.071

94.2nd 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	0.071 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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

An attacker could exploit this vulnerability by sending a crafted H.323 RAS packet through an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition. This vulnerability affects Cisco devices that are configured to use an application layer gateway with NAT (NAT ALG) for H.323 RAS messages. By default, a NAT ALG is enabled for H.323 RAS messages. Cisco Bug IDs: CSCvc57217.

Affected and fixed versions · 321 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	≥ 12.4 ≤ 15.6	after 15.6	NVD
1100-4g\6g integrated services router	—	no fixed version listed	NVD
1100-4g integrated services router	—	no fixed version listed	NVD
1100-4gltegb integrated services router	—	no fixed version listed	NVD
1100-4gltena integrated services router	—	no fixed version listed	NVD
1100-4p integrated services router	—	no fixed version listed	NVD
1100-6g integrated services router	—	no fixed version listed	NVD
1100-8p integrated services router	—	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-83rp-43rf-7hmv

NVD nvd.nist.gov/vuln/detail/CVE-2017-12231

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-3804

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-nat
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2017-12231

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