

CVE-2017-12240

Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

The DHCP relay subsystem of Cisco IOS 12.2 through 15.6 and Cisco IOS XE Software contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code and gain full control of an affected system. The attacker could also cause an affected system to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to a buffer overflow condition in the DHCP relay subsystem of the affected software.

EVRS 75_{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.138 96.5th 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	0.138 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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

An attacker could exploit this vulnerability by sending a crafted DHCP Version 4 (DHCPv4) packet to an affected system. A successful exploit could allow the attacker to execute arbitrary code and gain full control of the affected system or cause the affected system to reload, resulting in a DoS condition. Cisco Bug IDs: CSCsm45390, CSCuw77959.

Affected and fixed versions · 257 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	≥ 12.2 ≤ 15.6	after 15.6	NVD
1000 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-q8rh-r33q-hvj2

NVD nvd.nist.gov/vuln/detail/CVE-2017-12240

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-3813

Additional guidance quickview.cloudapps.cisco.com/quickview/bug/CSCsm45390

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

Current data evulnable.com/vulnerability-management/cve/CVE-2017-12240

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