

CVE-2018-0174

Cisco IOS Software and Cisco IOS XE Software Improper Input Validation Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

A vulnerability in the DHCP option 82 encapsulation functionality of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software performs incomplete input validation of option 82 information that it receives in DHCP Version 4 (DHCPv4) packets from DHCP relay agents.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 8.6 High · NVD	EPSS 0.076 94.5th percentile · FIRST	CISA DEADLINE Mar 17, 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	0.076 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.6	☐ 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 DHCPv4 packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Cisco Bug IDs: CSCuh91645.

Affected and fixed versions · 3 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	12.2\ (33\)sre7a ≤ 15.2\ (4a\)ea5 ≤ 15.2\ (6\)e0a	after 15.2\ (4a\)ea5 · after 15.2\ (6\)e0a	NVD
ios xe	12.2\ (33\)sre7a ≤ 15.2\ (4a\)ea5 ≤ 15.2\ (6\)e0a	after 15.2\ (4a\)ea5 · after 15.2\ (6\)e0a	NVD
7600 series route switch processor 720	—	no fixed version listed	NVD
7600 series supervisor engine 32	—	no fixed version listed	NVD
7600 series supervisor engine 720	—	no fixed version listed	NVD
allen-bradley stratix 8300	—	no fixed version listed	NVD
allen-bradley armorstratix 5700	—	no fixed version listed	NVD
allen-bradley stratix 5400	—	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-qcqh-fmx4-f33r

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-dhcpr3

NVD nvd.nist.gov/vuln/detail/CVE-2018-0174

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-0997

Current data evulnable.com/vulnerability-management/cve/CVE-2018-0174

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