

CVE-2018-0175

Cisco IOS, XR, and XE Software Buffer Overflow Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Format String vulnerability in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. Cisco Bug IDs: CSCvd73664.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.0 High · NVD	EPSS 0.035 89th 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	0.035 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.0	☐ 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 · 2 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	15.4\3\m4.1 ≤ 15.2\4a\ea5 ≤ 15.2\6\ea0a ≤ 15.6.3m1	after 15.2\4a\ea5 · after 15.2\6\ea0a · after 15.6.3m1	NVD
ios xe	15.4\3\m4.1 ≤ 15.2\4a\ea5 ≤ 15.2\6\ea0a ≤ 15.6.3m1	after 15.2\4a\ea5 · after 15.2\6\ea0a · after 15.6.3m1	NVD
ios xr	15.4\3\m4.1	no fixed version listed	NVD
allen-bradley stratix 8300 industrial managed ethernet switch	—	no fixed version listed	NVD
allen-bradley armorstratix 5700	—	no fixed version listed	NVD
allen-bradley stratix 5400	—	no fixed version listed	NVD
allen-bradley stratix 5410	—	no fixed version listed	NVD
allen-bradley stratix 5700	—	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-f6hc-7357-x73w

NVD nvd.nist.gov/vuln/detail/CVE-2018-0175

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-0998

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-lldp
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2018-0175

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