CVE-2017-12234

Cisco IOS Software Common Industrial Protocol Request Denial-of-Service Vulnerability

CISA KEV since Mar 3, 2022 | Actively exploited

Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature in Cisco IOS 12.4 through 15.6 could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of crafted CIP packets destined to an affected device. An attacker could exploit these vulnerabilities by sending crafted CIP packets to be processed by an affected device.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	7.5	0.071	Mar 24, 2022
Urgent priority	High · NVD	94.2nd percentile · FIRST	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

A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Cisco Bug IDs: CSCvc43709.

Affected and fixed versions · 47 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	⩾ 12.4 ⩽ 15.6	after 15.6	NVD
1000 integrated services router	–	no fixed version listed	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	–	no fixed version listed	NVD
1100-4p integrated services router	–	no fixed version listed	NVD

Sources

Vendor guidance	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-cip	**NVD**	nvd.nist.gov/vuln/detail/CVE-2017-12234
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	**ENISA EUVD**	euvd.enisa.europa.eu/vulnerability/EUVD-2017-3807
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-12234		

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