

CVE-2010-3035

Cisco IOS XR Border Gateway Protocol (BGP) Denial-of-Service Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Cisco IOS XR 3.4.0 through 3.9.1, when BGP is enabled, does not properly handle unrecognized transitive attributes, which allows remote attackers to cause a denial of service (peering reset) via a crafted prefix announcement, as demonstrated in the wild in August 2010 with attribute type code 99, aka Bug ID CSCti62211.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.057 93rd percentile · FIRST	CISA DEADLINE Apr 15, 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	0.057 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios xr	≥ 3.4.0 ≤ 3.9.1	after 3.9.1	NVD

Sources

Vendor guidance	exchange.xforce.ibmcloud.com/vulnerabilities/61443	NVD	nvd.nist.gov/vuln/detail/CVE-2010-3035
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2010-3037
Current data	evulnable.com/vulnerability-management/cve/CVE-2010-3035		

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