CVE-2009-2055

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 3.8.1 allows remote attackers to cause a denial of service (session reset) via a BGP UPDATE message with an invalid attribute, as demonstrated in the wild on 17 August 2009.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	5.9	0.033	Apr 15, 2022
Urgent priority	Medium · NVD	88.5th 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	0.033 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 5.9	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

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	no fixed version listed	NVD
	3.4.0		
	3.4.1		
	3.4.2		
	3.4.3		
	3.5		
	3.5.2		
	3.5.3		
	3.5.4		
	3.6.0		
	3.6.1		
	3.6.2		
	3.6.3		
	3.7.0		
	3.7.1		
	3.7.2		
	3.7.3		
	3.8.0		
	3.8.1		

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2009-2055

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2009-2051

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

Current data evulnable.com/vulnerability-management/cve/CVE-2009-2055

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