CVE-2009-2055

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-2055
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-19 17:30:01 UTC
Updated	2026-04-22 15:40:28 UTC
Description	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

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from ADP

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.007710000 probability, percentile 0.736300000 (date 2026-04-25)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-20 | n/a | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:N/A:P

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS XR
Name	Cisco IOS XR Border Gateway Protocol (BGP) Denial-of-Service Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2009-2055

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xr	3.4	All	All	All
Operating System	Cisco	Ios Xr	3.4.0	All	All	All
Operating System	Cisco	Ios Xr	3.4.1	All	All	All
Operating System	Cisco	Ios Xr	3.4.2	All	All	All
Operating System	Cisco	Ios Xr	3.4.3	All	All	All
Operating System	Cisco	Ios Xr	3.5	All	All	All
Operating System	Cisco	Ios Xr	3.5.2	All	All	All

Operating System	Cisco	Ios Xr	3.5.3	All	All	All
Operating System	Cisco	Ios Xr	3.5.4	All	All	All
Operating System	Cisco	Ios Xr	3.6.0	All	All	All
Operating System	Cisco	Ios Xr	3.6.1	All	All	All
Operating System	Cisco	Ios Xr	3.6.2	All	All	All
Operating System	Cisco	Ios Xr	3.6.3	All	All	All
Operating System	Cisco	Ios Xr	3.7.0	All	All	All
Operating System	Cisco	Ios Xr	3.7.1	All	All	All
Operating System	Cisco	Ios Xr	3.7.2	All	All	All
Operating System	Cisco	Ios Xr	3.7.3	All	All	All
Operating System	Cisco	Ios Xr	3.8.0	All	All	All
Operating System	Cisco	Ios Xr	3.8.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Anyone else seeing "(invalid or corrupt AS path) 3 bytes E01100" ?	af854a3a-2127-422b-91ae-364d
Cisco Security Advisory: Cisco IOS XR Software Border Gateway Protocol Vulnerabilities - Cisco Systems	af854a3a-2127-422b-91ae-364d
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467
Cisco IOS XR BGP Update Processing Flaw Lets Remote BGP Peers Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364d
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

379462 For Vulnerability CVE-2009-2055

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**