CVE-2015-4191

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

Summary

CVE	CVE-2015-4191
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-19 01:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco IOS XR 5.2.1 allows remote attackers to cause a denial of service (ipv6_io service reload) via a malformed IPv6 pack

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xr	5.2.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Cisco IOS XR IPv6 Packet Processing Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2
Cisco IOS XR IPv6 ipv6_io Service Processing Flaw Lets Remote Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da2
Cisco IOS XR Software CVE-2015-4191 Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.