CVE-2015-6301

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

Summary

CVE	CVE-2015-6301
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-20 14:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The DHCPv6 server in Cisco IOS on ASR 9000 devices with software 5.2.0 Base allows remote attackers to cause a denial

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
Hardware	Cisco	Asr 9001	-	All	All	All

Hardware	Cisco	Asr 9006	-	All	All	All
Hardware	Cisco	Asr 9010	-	All	All	All
Hardware	Cisco	Asr 9904	-	All	All	All
Hardware	Cisco	Asr 9912	-	All	All	All
Hardware	Cisco	Asr 9922	-	All	All	All
Operating System	Cisco	Ios Xr	5.2.0_base	All	All	All

Vendor Declared Affected Products

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

References

Reference
Cisco IOS for ASR 9000 Series Routers DHCPv6 Input Validation Flaw Lets Remote Users Cause the Target Service to Crash - SecurityTrack
Cisco ASR 9000 Series Aggregation Services Routers Denial of Service Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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