CVE-2015-6351

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

Summary

CVE	CVE-2015-6351
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-30 10:59:09 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco ASR 5500 System Architecture Evolution (SAE) Gateway devices with software 19.1.0.61559 and 19.2.0 allow remot

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-20 | 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
Application	Cisco	Asr 5000 Software	19.1.0.61559	All	All	All

Application	Cisco	Asr 5000 Software	19.2.0	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 ASR 5500 SAE Gateway BGP Denial of Service Vulnerability	af854a3a-2127-422b-91ae
Cisco ASR 5500 SAE Gateway Lets Remote Users Cause the Target BGP Process to Restart - SecurityTracker	af854a3a-2127-422b-91ae
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.