CVE-2015-6334

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

Summary

CVE	CVE-2015-6334
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-16 01:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco ASR 5000 and 5500 devices with software 18.0.0.57828 and 19.0.M0.61045 allow remote attackers to cause a denia

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
Operating System	Cisco	Asr 5000 Software	18.0.0.57828	All	All	All

Operating System	Cisco	Asr 5000 Software	19.0.m0.61045	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 Router TACACS Implementation Bug Lets Remote Users Cause the Target vpnmgr Service to Restart - SecurityTracker	af854a
Cisco ASR 5000 and ASR 5500 TACACS Denial of Service Vulnerability	af854a
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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