CVE-2012-5017

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

Summary

CVE	CVE-2012-5017
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-23 11:52:59 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco IOS before 15.1(1)SY1 allows remote authenticated users to cause a denial of service (device reload) by establishing

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 1001	-	All	All	All

Hardware	Cisco	Asr 1002	-	All	All	All
Hardware	Cisco	Asr 1002-x	-	All	All	All
Hardware	Cisco	Asr 1002 Fixed Router	-	All	All	All
Hardware	Cisco	Asr 1004	-	All	All	All
Hardware	Cisco	Asr 1006	-	All	All	All
Hardware	Cisco	Asr 1023 Router	-	All	All	All
Operating System	Cisco	Ios	15.1	All	All	All
Operating System	Cisco	Ios	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/release_...	af854a3a-2127-422b-91ae-364da2661108	www.cisco.cc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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