CVE-2012-4618

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

Summary

CVE	CVE-2012-4618
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-27 00:55:00 UTC
Updated	2013-04-11 03:31:00 UTC
Description	The SIP ALG feature in the NAT implementation in Cisco IOS 12.2, 12.4, and 15.0 through 15.2 allows remote attackers to

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	12.2	All	All	All
Operating System	Cisco	Ios	12.4	All	All	All
Operating System	Cisco	Ios	15.0	All	All	All
Operating System	Cisco	Ios	15.0(1)se	All	All	All
Operating System	Cisco	Ios	15.0\(1\)se	All	All	All
Operating System	Cisco	Ios	15.1	All	All	All
Operating System	Cisco	Ios	15.2	All	All	All
Operating System	Cisco	Ios	12.2	All	All	All
Operating System	Cisco	Ios	12.4	All	All	All
Operating System	Cisco	Ios	15.0	All	All	All
Operating System	Cisco	Ios	15.0\(1\)se	All	All	All
Operating System	Cisco	Ios	15.1	All	All	All
Operating System	Cisco	Ios	15.2	All	All	All

References

Reference	Source	Link	Tags
Cisco IOS NAT Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com	

Cisco IOS NAT Functionality CVE-2012-4618 Denial of Service Vulnerability	BID	www.securityfocus.com	
Cisco Security Advisory: Cisco IOS Software Network Address Translation Vulnerabilities	CISCO	tools.cisco.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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