CVE-2015-0712

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

Summary

CVE	CVE-2015-0712
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-01 10:59:00 UTC
Updated	2015-09-10 16:08:00 UTC
Description	The session-manager service in Cisco StarOS 12.0, 12.2(300), 14.0, and 14.0(600) on ASR 5000 devices allows remote at

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 5000	-	All	All	All
Hardware	Cisco	Asr 5000	-	All	All	All
Hardware	Cisco	Asr 5500	-	All	All	All
Hardware	Cisco	Asr 5500	-	All	All	All
Hardware	Cisco	Asr 5700	-	All	All	All
Hardware	Cisco	Asr 5700	-	All	All	All
Operating System	Cisco	Staros	12.0	All	All	All
Operating System	Cisco	Staros	12.2(300)	All	All	All
Operating System	Cisco	Staros	12.2\(300\)	All	All	All
Operating System	Cisco	Staros	14.0	All	All	All
Operating System	Cisco	Staros	14.0(600)	All	All	All
Operating System	Cisco	Staros	14.0\(600\)	All	All	All
Operating System	Cisco	Staros	12.0	All	All	All
Operating System	Cisco	Staros	12.2\(300\)	All	All	All
Operating System	Cisco	Staros	14.0	All	All	All
Operating System	Cisco	Staros	14.0\(600\)	All	All	All

References

Reference	Source
Cisco StarOS for Cisco ASR 5000 Series HTTP Packet Processing Denial of Service Vulnerability	CISCO
Cisco StarOS for Cisco ASR 5000 Series Router HTTP Processing Bug Lets Remote Users Deny Service - SecurityTracker	SECTRACK
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.