CVE-2014-0669

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

Summary

CVE	CVE-2014-0669
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-22 05:22:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The Wireless Session Protocol (WSP) feature in the Gateway GPRS Support Node (GGSN) component on Cisco ASR 500

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Asr 5000 Series Software	-	All	All	All
Application	Cisco	Asr 5000 Series Software	-	All	All	All

References

Reference	Source
Cisco Security Notice: Cisco ASR 5000 Series Gateway GPRS Support Node Traffic Bypass Vulnerability	CISCO
102318	OSVDB
Cisco ASR 5000 Series Gateway WSP Processing Bug Lets Remote Users Bypass Network Access Controls - SecurityTracker	SECTRACK
IBM X-Force Exchange	XF
Cisco ASR 5000 Series Devices GPRS Support Node Security Bypass Vulnerability	BID
Security Advisory SA56546 - Cisco Aggregation Services Routers (ASR) 5000 Series Security Bypass Vulnerability - Secunia	SECUNIA
tools.cisco.com/security/center/viewAlert.x	CONFIRM
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**