



CVE-2017-12217

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-12217
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-07 21:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the General Packet Radio Service (GPRS) Tunneling Protocol ingress packet handler of Cisco ASR 5500

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 5500	-	All	All	All
Hardware	Cisco	Asr 5500	-	All	All	All
Operating System	Cisco	Asr 5500 Firmware	-	All	All	All
Operating System	Cisco	Asr 5500 Firmware	-	All	All	All

References

Reference	
Cisco ASR 5500 System Architecture Evolution Gateway GPRS Tunneling Protocol Denial of Service Vulnerability	C
Cisco ASR 5500 Series SAE Gateways GPRS Processing Bug Lets Remote Users Cause the Target Service to Restart - SecurityTracker	S
Cisco ASR 5500 System Architecture Evolution Gateway CVE-2017-12217 Denial of Service Vulnerability	B
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)