



CVE-2016-9203

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

Summary

CVE	CVE-2016-9203
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-14 00:59:00 UTC
Updated	2016-12-22 21:11:00 UTC
Description	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco ASR 5000 Series Software could allow an un

Risk And Classification

Problem Types: CWE-119

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
Application	Cisco	Asr 5000 Series Software	20.0.2.3.65026	All	All	All
Application	Cisco	Asr 5000 Series Software	20.0.2.3.65026	All	All	All

References

Reference	Source
Cisco ASR 5000 Series IKEv2 Denial of Service Vulnerability	C
Cisco ASR 5000 Series Software CVE-2016-9203 Denial of Service Vulnerability	E
Cisco ASR 5000 Series Router IKEv2 Race Condition Lets Remote Users Cause the Target 'ipsecmgr' Service to Crash - SecurityTracker	S
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](#).

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