



CVE-2017-6672

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

Summary

CVE	CVE-2017-6672
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-25 19:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A vulnerability in certain filtering mechanisms of access control lists (ACLs) for Cisco ASR 5000 Series Aggregation Service

Risk And Classification

Problem Types: CWE-863

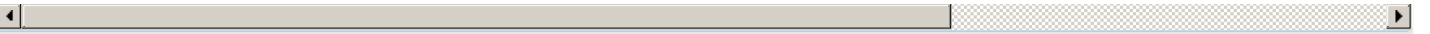
NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Asr 5000 Series Software	19.3.11	All	All	All
Application	Cisco	Asr 5000 Series Software	19.3.12	All	All	All
Application	Cisco	Asr 5000 Series Software	19.3.5	All	All	All
Application	Cisco	Asr 5000 Series Software	19.6.0	All	All	All
Application	Cisco	Asr 5000 Series Software	19.6.3	All	All	All
Application	Cisco	Asr 5000 Series Software	19.6.6	All	All	All
Application	Cisco	Asr 5000 Series Software	20.1.v5	All	All	All
Application	Cisco	Asr 5000 Series Software	20.2.12	All	All	All
Application	Cisco	Asr 5000 Series Software	20.2.4	All	All	All
Application	Cisco	Asr 5000 Series Software	20.3.0	All	All	All
Application	Cisco	Asr 5000 Series Software	20.3.1	All	All	All
Application	Cisco	Asr 5000 Series Software	21.0.v1.66638	All	All	All
Application	Cisco	Asr 5000 Series Software	21.0.v2	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.0	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.2	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65710	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65921	All	All	All

Application	Cisco	Asr 5000 Series Software	21.1.m0.65931	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65986	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.v0	All	All	All
Application	Cisco	Asr 5000 Series Software	21.2.a0.65914	All	All	All
Application	Cisco	Asr 5000 Series Software	21.2.a0.65995	All	All	All
Application	Cisco	Asr 5000 Series Software	21.3.0	All	All	All
Application	Cisco	Asr 5000 Series Software	19.3.11	All	All	All
Application	Cisco	Asr 5000 Series Software	19.3.12	All	All	All
Application	Cisco	Asr 5000 Series Software	19.3.5	All	All	All
Application	Cisco	Asr 5000 Series Software	19.6.0	All	All	All
Application	Cisco	Asr 5000 Series Software	19.6.3	All	All	All
Application	Cisco	Asr 5000 Series Software	19.6.6	All	All	All
Application	Cisco	Asr 5000 Series Software	20.1.v5	All	All	All
Application	Cisco	Asr 5000 Series Software	20.2.12	All	All	All
Application	Cisco	Asr 5000 Series Software	20.2.4	All	All	All
Application	Cisco	Asr 5000 Series Software	20.3.0	All	All	All
Application	Cisco	Asr 5000 Series Software	20.3.1	All	All	All
Application	Cisco	Asr 5000 Series Software	21.0.v1.66638	All	All	All
Application	Cisco	Asr 5000 Series Software	21.0.v2	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.0	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.2	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65710	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65921	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65931	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.m0.65986	All	All	All
Application	Cisco	Asr 5000 Series Software	21.1.v0	All	All	All
Application	Cisco	Asr 5000 Series Software	21.2.a0.65914	All	All	All
Application	Cisco	Asr 5000 Series Software	21.2.a0.65995	All	All	All
Application	Cisco	Asr 5000 Series Software	21.3.0	All	All	All

References

Reference	Source	Lin
Cisco ASR 5000 Series Aggregation Services Router CVE-2017-6672 Security Bypass Vulnerability	BID	ww
Cisco ASR 5000 Series Router Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker	SECTRACK	ww
Cisco ASR 5000 Series Aggregation Services Routers Access Control List Security Bypass Vulnerability	CONFIRM	too



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](#)