



CVE-2015-0672

Published on: 03/26/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:19 PM UTC

CVE-2015-0672

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Asr 9001](#) from [Cisco](#) contain the following vulnerability:

The DHCPv4 server in Cisco IOS XR 5.2.2 on ASR 9000 devices allows remote attackers to cause a denial of service (service outage) via a flood of crafted DHCP packets, aka Bug ID CSCup67822.

CVE-2015-0672 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

Cisco IOS XR Software DHCPv4 Server Denial of Service Vulnerability

[Vendor Advisory](#)
[tools.cisco.com](#)
[text/html](#)

[CISCO 20150324 Cisco IOS XR Software DHCPv4 Server Denial of Service Vulnerability](#)

Cisco 9000 Series Aggregation Services Routers DHCPv4 Processing Flaw Lets Remote Users Deny Service - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTRAK 1031970](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Cisco	Asr 9001	-	All	All	All
Hardware  	Cisco	Asr 9001	-	All	All	All
Hardware  	Cisco	Asr 9006	-	All	All	All
Hardware  	Cisco	Asr 9006	-	All	All	All
Hardware  	Cisco	Asr 9010	-	All	All	All
Hardware  	Cisco	Asr 9010	-	All	All	All
Hardware  	Cisco	Asr 9904	-	All	All	All
Hardware  	Cisco	Asr 9904	-	All	All	All
Hardware  	Cisco	Asr 9912	-	All	All	All
Hardware  	Cisco	Asr 9912	-	All	All	All
Hardware  	Cisco	Asr 9922	-	All	All	All
Hardware  	Cisco	Asr 9922	-	All	All	All
Operating System	Cisco	Ios Xr	5.2.2	All	All	All
Operating System	Cisco	Ios Xr	5.2.2	All	All	All
cpe:2.3:h:cisco:asr_9001:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9001:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9006:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9006:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9010:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9010:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9904:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9904:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9912:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9912:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9922:-:*****.*.*.*.						
cpe:2.3:h:cisco:asr_9922:-:*****.*.*.*.						
cpe:2.3:o:cisco:ios_xr:5.2.2:*.*.*.*.*.*.*.*.						

cpe:2.3:o:cisco:ios_xr:5.2.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

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](#)