

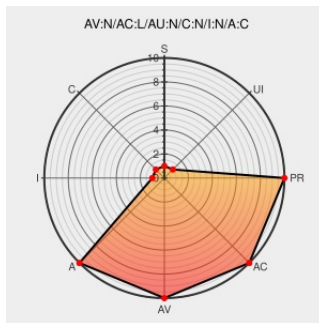


CVE-2015-6272

Published on: 08/31/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6272

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Asr 1001](#) from [Cisco](#) contain the following vulnerability:

Cisco IOS XE 2.1.0 through 2.2.3 and 2.3.0 on ASR 1000 devices, when NAT Application Layer Gateway is used, allows remote attackers to cause a denial of service (Embedded Services Processor crash) via a crafted H.323 packet, aka Bug ID CSCsx35393, CSCsx07094, and CSCsw93064.

CVE-2015-6272 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Cisco ASR 1000 Series Aggregation Services Routers Crafted H.323 Packet Denial of Service Vulnerabilities

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

[CISCO 20150827 Cisco ASR 1000 Series Aggregation Services Routers Crafted H.323 Packet Denial of Service Vulnerabilities](#)

Cisco ASR 1000 Series Router L2TP/IPv4/IPv6/SIP/H.323 Processing Bugs Let Remote Users Cause the Target System to Crash - SecurityTracker

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

[SECTrack 1033410](#)

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 1001	-	All	All	All
Hardware  	Cisco	Asr 1001	-	All	All	All
Hardware  	Cisco	Asr 1001-x	-	All	All	All
Hardware  	Cisco	Asr 1001-x	-	All	All	All
Hardware  	Cisco	Asr 1002	-	All	All	All
Hardware  	Cisco	Asr 1002	-	All	All	All
Hardware  	Cisco	Asr 1002-x	-	All	All	All
Hardware  	Cisco	Asr 1002-x	-	All	All	All
Hardware  	Cisco	Asr 1004	-	All	All	All
Hardware  	Cisco	Asr 1004	-	All	All	All
Hardware  	Cisco	Asr 1006	-	All	All	All
Hardware  	Cisco	Asr 1006	-	All	All	All
Hardware  	Cisco	Asr 1013	-	All	All	All
Hardware  	Cisco	Asr 1013	-	All	All	All
Operating System	Cisco	ios Xe	2.1.0	All	All	All
Operating System	Cisco	ios Xe	2.1.1	All	All	All
Operating System	Cisco	ios Xe	2.1.2	All	All	All
Operating System	Cisco	ios Xe	2.1.3	All	All	All
Operating System	Cisco	ios Xe	2.2.1	All	All	All
Operating System	Cisco	ios Xe	2.2.2	All	All	All
Operating System	Cisco	ios Xe	2.2.3	All	All	All
Operating System	Cisco	ios Xe	2.3.0	All	All	All
Operating System	Cisco	ios Xe	2.1.0	All	All	All
Operating System	Cisco	ios Xe	2.1.1	All	All	All

Operating System	Cisco	Ios Xe	2.1.2	All	All	All
Operating System	Cisco	Ios Xe	2.1.3	All	All	All
Operating System	Cisco	Ios Xe	2.2.1	All	All	All
Operating System	Cisco	Ios Xe	2.2.2	All	All	All
Operating System	Cisco	Ios Xe	2.2.3	All	All	All
Operating System	Cisco	Ios Xe	2.3.0	All	All	All
cpe:2.3:h:cisco:asr_1001:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1001:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1001-x:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1001-x:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1002:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1002:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1002-x:-:*:*:*:*:*:						
cpe:2.3:h:cisco:asr_1002-x:-:*:*:*:*::~:						
cpe:2.3:h:cisco:asr_1004:-:*:*:*:*::~:						
cpe:2.3:h:cisco:asr_1004:-:*:*:*:*:::						
cpe:2.3:h:cisco:asr_1006:-:*:*:*:*:::						
cpe:2.3:h:cisco:asr_1006:-:*:*:*:*:::						
cpe:2.3:h:cisco:asr_1013:-:*:*:*:*:::						
cpe:2.3:h:cisco:asr_1013:-:*:*:*:*:::						
cpe:2.3:o:cisco:ios_xe:2.1.0:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:2.1.1:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:2.1.2:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:2.1.3:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:2.2.1:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:2.2.2:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:2.2.3:*:*:*:*:*:						

cpe:2.3:o:cisco:ios_xe:2.3.0:*****:
cpe:2.3:o:cisco:ios_xe:2.1.0:*****:
cpe:2.3:o:cisco:ios_xe:2.1.1:*****:
cpe:2.3:o:cisco:ios_xe:2.1.2:*****:
cpe:2.3:o:cisco:ios_xe:2.1.3:*****:
cpe:2.3:o:cisco:ios_xe:2.2.1:*****:
cpe:2.3:o:cisco:ios_xe:2.2.2:*****:
cpe:2.3:o:cisco:ios_xe:2.2.3:*****:
cpe:2.3:o:cisco:ios_xe:2.3.0:*****:

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](#)