



# CVE-2014-3335

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-3335
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-08-26 10:55:00 UTC
<b>Updated</b>	2017-08-29 01:34:00 UTC
<b>Description</b>	Cisco IOS XR 4.3(.2) and earlier on ASR 9000 devices does not properly perform NetFlow sampling of packets with multica

## Risk And Classification

**Problem Types: CWE-20**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 9000 Rsp440 Router	-	All	All	All
Hardware	Cisco	Asr 9000 Rsp440 Router	-	All	All	All
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	4.3.0	All	All	All
Operating System	Cisco	ios Xr	4.3.1	All	All	All
Operating System	Cisco	ios Xr	4.3.0	All	All	All

Operating System	<a href="#">Cisco</a>	<a href="#">Ios Xr</a>	4.3.1	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Ios Xr</a>	All	All	All	All

## References

### Reference

Cisco Security Notice: Cisco IOS XR Software Packet Parsing Denial of Service Vulnerability

[tools.cisco.com/security/center/viewAlert.x](https://tools.cisco.com/security/center/viewAlert.x)

Cisco ASR 9000 Series IOS XR Router Packet Processing Flaw Lets Remote Users Deny Service - SecurityTracker

IBM X-Force Exchange

Cisco IOS XR Software Packet Parsing CVE-2014-3335 Denial of Service Vulnerability

Security Advisory SA60222 - Cisco IOS XR Software NetFlow Multicast MAC Address Processing Denial of Service Vulnerability - Secunia

CVE Program record

NVD vulnerability detail



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](#)