



CVE-2014-0614

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

Summary

CVE	CVE-2014-0614
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-14 15:09:00 UTC
Updated	2014-04-15 13:30:00 UTC
Description	Juniper Junos 13.2 before 13.2R3 and 13.3 before 13.3R1, when PIM is enabled, allows remote attackers to cause a denial of service (CPU usage spike) via a crafted IGMP packet.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	13.2	All	All	All
Operating System	Juniper	Junos	13.3	All	All	All
Operating System	Juniper	Junos	13.2	All	All	All
Operating System	Juniper	Junos	13.3	All	All	All

References

Reference	Source
Security Advisory SA57819 - Juniper JunOS IGMP Packet Processing Denial of Service Vulnerability - Secunia	SECUNIA
2014-04 Security Bulletin: Junos: Kernel panic processing high rate of crafted IGMP packets (CVE-2014-0614) - Juniper Networks	CONFIRMED
Juniper Junos IGMP Processing Flaw Lets Remote Users Deny Service - SecurityTracker	SECURITYTRACKER
Juniper Junos CVE-2014-0614 Denial of Service Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

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