



CVE-2017-2300

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

Summary

CVE	CVE-2017-2300
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-30 14:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	On Juniper Networks SRX Series Services Gateways chassis clusters running Junos OS 12.1X46 prior to 12.1X46-D65, 12

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	All	d60	All	All
Operating System	Juniper	Junos	All	d35	All	All
Operating System	Juniper	Junos	All	d50	All	All

References

Reference

- Juniper Junos CVE-2017-2300 Denial of Service Vulnerability
- Juniper Junos SRX Series Services Gateway Multicast Processing Flaw Lets Remote Users Cause the Target Service to Crash - SecurityTrac
- 2017-01 Security Bulletin: Junos: SRX Series denial of service vulnerability in flowd due to crafted multicast packets (CVE-2017-2300) - Juniper
- 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](#).

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

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