



CVE-2023-4481

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

Summary

CVE	CVE-2023-4481
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-01 00:15:00 UTC
Updated	2023-09-07 19:11:00 UTC
Description	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos C

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	All	All	All	All
Operating System	Juniper	Junos Os Evolved	All	All	All	All

References

Reference	Source	Link	Tags
BGP Error Messages Junos OS Juniper Networks	MISC	www.juniper.net	
RFC 4271: A Border Gateway Protocol 4 (BGP-4)	MISC	www.rfc-editor.org	
RFC 7606: Revised Error Handling for BGP UPDATE Messages	MISC	www.rfc-editor.org	
CEC Juniper Community	MISC	kb.juniper.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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