



CVE-2018-0037

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

Summary

CVE	CVE-2018-0037
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-11 18:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	Junos OS routing protocol daemon (RPD) process may crash and restart or may lead to remote code execution while process

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	15.1	f2	All	All
Operating System	Juniper	Junos	15.1	f5-s7	All	All
Operating System	Juniper	Junos	15.1	f6	All	All
Operating System	Juniper	Junos	15.1	f6-s3	All	All
Operating System	Juniper	Junos	15.1	f7	All	All
Operating System	Juniper	Junos	15.1	r3	All	All
Operating System	Juniper	Junos	15.1	r5	All	All
Operating System	Juniper	Junos	15.1	r7	All	All
Operating System	Juniper	Junos	15.1	f2	All	All
Operating System	Juniper	Junos	15.1	f5-s7	All	All
Operating System	Juniper	Junos	15.1	f6	All	All
Operating System	Juniper	Junos	15.1	f6-s3	All	All
Operating System	Juniper	Junos	15.1	f7	All	All
Operating System	Juniper	Junos	15.1	r3	All	All
Operating System	Juniper	Junos	15.1	r5	All	All
Operating System	Juniper	Junos	15.1	r7	All	All

References

Reference

2018-07 Security Bulletin: Junos OS: RPD daemon crashes due to receipt of crafted BGP NOTIFICATION messages (CVE-2018-0037) - Juniper Networks

Juniper Junos BGP NOTIFICATION Processing Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Internet2

LEGACY: The Indiana University GlobalNOC

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](#)