



CVE-2022-22220

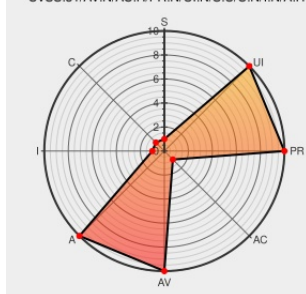
Published on: Not Yet Published

Last Modified on: 10/20/2022 08:21:00 PM UTC

CVE-2022-22220 - advisory for JSA69902

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Junos](#) from [Juniper](#) contain the following vulnerability:

A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Routing Protocol Daemon (rpd) of Juniper Networks Junos OS, Junos OS Evolved allows a network-based unauthenticated attacker to cause a Denial of Service (DoS). When a BGP flow route with redirect IP extended community is received, and the reachability to the next-

hop of the corresponding redirect IP is flapping, the rpd process might crash. Whether the crash occurs depends on the timing of the internally processing of these two events and is outside the attackers control. Please note that this issue also affects Route-Reflectors unless 'routing-options flow firewall-install-disable' is configured. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.4 versions prior to 19.4R3-S8; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1.

CVE-2022-22220 has been assigned by [J](#) sirt@juniper.net to track the vulnerability - currently rated as **MEDIUM** severity.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

Vulnerability Patch/Work Around

There are no viable workarounds for this issue.

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact

impact		impact		impact		
UNCHANGED		NONE		NONE		HIGH
CVE References						
Description		Tags		Link		
CEC Juniper Community		kb.juniper.net text/html		 CONFIRM kb.juniper.net/JSA69902		
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	All	All	All	All
Operating System	Juniper	Junos	18.4	-	All	All
Operating System	Juniper	Junos	18.4	r1	All	All
Operating System	Juniper	Junos	18.4	r1-s1	All	All
Operating System	Juniper	Junos	18.4	r1-s2	All	All
Operating System	Juniper	Junos	18.4	r1-s3	All	All
Operating System	Juniper	Junos	18.4	r1-s4	All	All
Operating System	Juniper	Junos	18.4	r1-s5	All	All
Operating System	Juniper	Junos	18.4	r1-s6	All	All
Operating System	Juniper	Junos	18.4	r1-s7	All	All
Operating System	Juniper	Junos	18.4	r2	All	All
Operating System	Juniper	Junos	18.4	r2-s1	All	All
Operating System	Juniper	Junos	18.4	r2-s2	All	All
Operating System	Juniper	Junos	18.4	r2-s3	All	All

Operating System	Juniper	Junos	18.4	r2-s4	All	All
Operating System	Juniper	Junos	18.4	r2-s5	All	All
Operating System	Juniper	Junos	18.4	r2-s6	All	All
Operating System	Juniper	Junos	18.4	r2-s7	All	All
Operating System	Juniper	Junos	18.4	r2-s8	All	All
Operating System	Juniper	Junos	18.4	r2-s9	All	All
Operating System	Juniper	Junos	18.4	r3-s10	All	All
Operating System	Juniper	Junos	19.1	-	All	All
Operating System	Juniper	Junos	19.1	r1	All	All
Operating System	Juniper	Junos	19.1	r1-s1	All	All
Operating System	Juniper	Junos	19.1	r1-s2	All	All
Operating System	Juniper	Junos	19.1	r1-s3	All	All
Operating System	Juniper	Junos	19.1	r1-s4	All	All
Operating System	Juniper	Junos	19.1	r1-s5	All	All
Operating System	Juniper	Junos	19.1	r1-s6	All	All
Operating System	Juniper	Junos	19.1	r2	All	All
Operating System	Juniper	Junos	19.1	r2-s1	All	All
Operating System	Juniper	Junos	19.1	r2-s2	All	All
Operating System	Juniper	Junos	19.1	r2-s3	All	All
Operating System	Juniper	Junos	19.1	r3	All	All
Operating System	Juniper	Junos	19.1	r3-s1	All	All
Operating System	Juniper	Junos	19.1	r3-s2	All	All
Operating System	Juniper	Junos	19.1	r3-s3	All	All

Operating System	Juniper	Junos	19.1	r3-s4	All	All
Operating System	Juniper	Junos	19.1	r3-s5	All	All
Operating System	Juniper	Junos	19.1	r3-s6	All	All
Operating System	Juniper	Junos	19.4	-	All	All
Operating System	Juniper	Junos	19.4	r1	All	All
Operating System	Juniper	Junos	19.4	r1-s1	All	All
Operating System	Juniper	Junos	19.4	r1-s2	All	All
Operating System	Juniper	Junos	19.4	r1-s3	All	All
Operating System	Juniper	Junos	19.4	r1-s4	All	All
Operating System	Juniper	Junos	19.4	r2	All	All
Operating System	Juniper	Junos	19.4	r2-s1	All	All
Operating System	Juniper	Junos	19.4	r2-s2	All	All
Operating System	Juniper	Junos	19.4	r2-s3	All	All
Operating System	Juniper	Junos	19.4	r2-s4	All	All
Operating System	Juniper	Junos	19.4	r2-s5	All	All
Operating System	Juniper	Junos	19.4	r3-s6	All	All
Operating System	Juniper	Junos	19.4	r3-s7	All	All
Operating System	Juniper	Junos	20.2	-	All	All
Operating System	Juniper	Junos	20.2	r1	All	All
Operating System	Juniper	Junos	20.2	r1-s1	All	All
Operating System	Juniper	Junos	20.2	r1-s2	All	All
Operating System	Juniper	Junos	20.2	r1-s3	All	All
Operating System	Juniper	Junos	20.2	r2	All	All

Operating System	Juniper	Junos	20.2	r2-s1	All	All
Operating System	Juniper	Junos	20.2	r2-s2	All	All
Operating System	Juniper	Junos	20.2	r2-s3	All	All
Operating System	Juniper	Junos	20.2	r3	All	All
Operating System	Juniper	Junos	20.2	r3-s1	All	All
Operating System	Juniper	Junos	20.2	r3-s2	All	All
Operating System	Juniper	Junos	20.3	-	All	All
Operating System	Juniper	Junos	20.3	r1	All	All
Operating System	Juniper	Junos	20.3	r1-s1	All	All
Operating System	Juniper	Junos	20.3	r1-s2	All	All
Operating System	Juniper	Junos	20.3	r2	All	All
Operating System	Juniper	Junos	20.3	r2-s1	All	All
Operating System	Juniper	Junos	20.3	r3	All	All
Operating System	Juniper	Junos	20.3	r3-s1	All	All
Operating System	Juniper	Junos	20.3	r3-s2	All	All
Operating System	Juniper	Junos	20.4	-	All	All
Operating System	Juniper	Junos	20.4	r1	All	All
Operating System	Juniper	Junos	20.4	r1-s1	All	All
Operating System	Juniper	Junos	20.4	r2	All	All
Operating System	Juniper	Junos	20.4	r2-s1	All	All
Operating System	Juniper	Junos	20.4	r2-s2	All	All
Operating System	Juniper	Junos	21.1	-	All	All
Operating System	Juniper	Junos	21.1	r1	All	All

Operating System	Juniper	Junos	21.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	All	All	All	All
Operating System	Juniper	Junos Os Evolved	20.4	-	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	-	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1-s1	All	All
cpe:2.3:o:juniper:junos:*.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:-.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s1:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s2:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s3:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s4:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s5:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s6:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r1-s7:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2-s1:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2-s2:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2-s3:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2-s4:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2-s5:.*.*.*.*.*.*.*:						
cpe:2.3:o:juniper:junos:18.4:r2-s6:.*.*.*.*.*.*.*:						

cpe:2.3:o:juniper:junos:18.4:r2-s7:*****:
cpe:2.3:o:juniper:junos:18.4:r2-s8:*****:
cpe:2.3:o:juniper:junos:18.4:r2-s9:*****:
cpe:2.3:o:juniper:junos:18.4:r3-s10:*****:
cpe:2.3:o:juniper:junos:19.1:-:*****:
cpe:2.3:o:juniper:junos:19.1:r1:*****:
cpe:2.3:o:juniper:junos:19.1:r1-s1:*****:
cpe:2.3:o:juniper:junos:19.1:r1-s2:*****:
cpe:2.3:o:juniper:junos:19.1:r1-s3:*****:
cpe:2.3:o:juniper:junos:19.1:r1-s4:*****:
cpe:2.3:o:juniper:junos:19.1:r1-s5:*****:
cpe:2.3:o:juniper:junos:19.1:r1-s6:*****:
cpe:2.3:o:juniper:junos:19.1:r2:*****:
cpe:2.3:o:juniper:junos:19.1:r2-s1:*****:
cpe:2.3:o:juniper:junos:19.1:r2-s2:*****:
cpe:2.3:o:juniper:junos:19.1:r2-s3:*****:
cpe:2.3:o:juniper:junos:19.1:r3:*****:
cpe:2.3:o:juniper:junos:19.1:r3-s1:*****:
cpe:2.3:o:juniper:junos:19.1:r3-s2:*****:
cpe:2.3:o:juniper:junos:19.1:r3-s3:*****:
cpe:2.3:o:juniper:junos:19.1:r3-s4:*****:
cpe:2.3:o:juniper:junos:19.1:r3-s5:*****:
cpe:2.3:o:juniper:junos:19.1:r3-s6:*****:
cpe:2.3:o:juniper:junos:19.4:-:*****:
cpe:2.3:o:juniper:junos:19.4:r1:*****:
cpe:2.3:o:juniper:junos:19.4:r1-s1:*****:
cpe:2.3:o:juniper:junos:19.4:r1-s2:*****:
cpe:2.3:o:juniper:junos:19.4:r1-s3:*****:
cpe:2.3:o:juniper:junos:19.4:r1-s4:*****:

cpe:2.3:o:juniper:junos:19.4:r2:~::~:
cpe:2.3:o:juniper:junos:19.4:r2-s1:~::~:
cpe:2.3:o:juniper:junos:19.4:r2-s2:~::~:
cpe:2.3:o:juniper:junos:19.4:r2-s3:~::~:
cpe:2.3:o:juniper:junos:19.4:r2-s4:~::~:
cpe:2.3:o:juniper:junos:19.4:r2-s5:~::~:
cpe:2.3:o:juniper:junos:19.4:r3-s6:~::~:
cpe:2.3:o:juniper:junos:19.4:r3-s7:~::~:
cpe:2.3:o:juniper:junos:20.2:-:~::~:
cpe:2.3:o:juniper:junos:20.2:r1:~::~:
cpe:2.3:o:juniper:junos:20.2:r1-s1:~::~:
cpe:2.3:o:juniper:junos:20.2:r1-s2:~::~:
cpe:2.3:o:juniper:junos:20.2:r1-s3:~::~:
cpe:2.3:o:juniper:junos:20.2:r2:~::~:
cpe:2.3:o:juniper:junos:20.2:r2-s1:~::~:
cpe:2.3:o:juniper:junos:20.2:r2-s2:~::~:
cpe:2.3:o:juniper:junos:20.2:r2-s3:~::~:
cpe:2.3:o:juniper:junos:20.2:r3:~::~:
cpe:2.3:o:juniper:junos:20.2:r3-s1:~::~:
cpe:2.3:o:juniper:junos:20.2:r3-s2:~::~:
cpe:2.3:o:juniper:junos:20.3:-:~::~:
cpe:2.3:o:juniper:junos:20.3:r1:~::~:
cpe:2.3:o:juniper:junos:20.3:r1-s1:~::~:
cpe:2.3:o:juniper:junos:20.3:r1-s2:~::~:
cpe:2.3:o:juniper:junos:20.3:r2:~::~:
cpe:2.3:o:juniper:junos:20.3:r2-s1:~::~:
cpe:2.3:o:juniper:junos:20.3:r3:~::~:
cpe:2.3:o:juniper:junos:20.3:r3-s1:~::~:

cpe:2.3:o:juniper:junos:20.3:r3-s2:~::~::~::~:
cpe:2.3:o:juniper:junos:20.4:-:~::~::~::~:
cpe:2.3:o:juniper:junos:20.4:r1:~::~::~::~:
cpe:2.3:o:juniper:junos:20.4:r1-s1:~::~::~::~:
cpe:2.3:o:juniper:junos:20.4:r2:~::~::~::~:
cpe:2.3:o:juniper:junos:20.4:r2-s1:~::~::~::~:
cpe:2.3:o:juniper:junos:20.4:r2-s2:~::~::~::~:
cpe:2.3:o:juniper:junos:21.1:-:~::~::~::~:
cpe:2.3:o:juniper:junos:21.1:r1:~::~::~::~:
cpe:2.3:o:juniper:junos:21.1:r1-s1:~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:20.4:-:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r1:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r1-s1:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r1-s2:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:21.1:-:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:21.1:r1:~::~::~::~::~:
cpe:2.3:o:juniper:junos_os_evolved:21.1:r1-s1:~::~::~::~::~:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @sidfm_jp	Juniper Networks Junos OS の BGP の処理にサービスが妨害される問題 (CVE-2022-22220) [43629] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2022-10-17 09:00:10
 @CVEreport	CVE-2022-22220 : A Time-of-check Time-of-use TOCTOU Race Condition vulnerability in Routing Protocol Daemon rpd... twitter.com/i/web/status/1...	2022-10-18 02:54:21

[← Previous ID](#)

Next ID→

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](#)