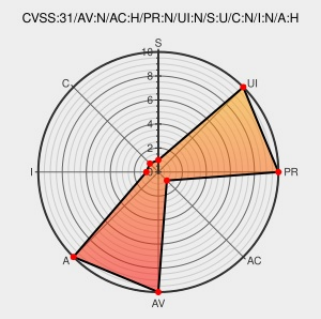
CVE-2022-22213

Published on: Not Yet Published

Last Modified on: 07/29/2022 10:46:00 PM UTC

CVE-2022-22213 - advisory for JSA69717

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Junos from Juniper contain the following vulnerability:

A vulnerability in Handling of Undefined Values in the routing protocol daemon (RPD) process of Juniper Networks Junos OS and Junos OS Evolved may allow an unauthenticated network-based attacker to crash the RPD process by sending a specific BGP update while the system is under heavy load, leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Malicious exploitation of this issue requires a very specific combination of load, timing, and configuration of the vulnerable system which is beyond the direct control of the attacker. Internal reproduction has only been possible through artificially created load and specially instrumented source code. Systems are only vulnerable to this issue if BGP multipath is enabled. Routers not configured for BGP multipath are not vulnerable to this issue. This issue affects: Juniper Networks Junos OS: 21.1 versions prior to 21.1R3-S1; 21.2 versions prior to 21.2R2-S2, 21.2R3; 21.3 versions prior to 21.3R2, 21.3R3; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved: 21.1 versions prior to 21.1R3-S1-EVO; 21.2 version 21.2R1-EVO and later versions; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.1. Juniper Networks Junos OS Evolved versions prior to 21.1-EVO.

CVE-2022-22213 has been assigned by 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

Disable BGP multipath, or configure 'set protocols bgp multipath-build deferred'.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction

NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
CEC Juniper Community	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA69717

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	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	21.1	r2	All	All
Operating System	Juniper	Junos	21.1	r2-s1	All	All
Operating System	Juniper	Junos	21.1	r2-s2	All	All
Operating System	Juniper	Junos	21.1	r3	All	All
Operating System	Juniper	Junos	21.2	-	All	All
Operating System	Juniper	Junos	21.2	r1	All	All
Operating System	Juniper	Junos	21.2	r1-s1	All	All
Operating System	Juniper	Junos	21.2	r1-s2	All	All
Operating System	Juniper	Junos	21.2	r2	All	All
Operating System	Juniper	Junos	21.2	r2-s1	All	All

System						
Operating System	Juniper	Junos	21.2	r2-s2	All	All
Operating System	Juniper	Junos	21.3	-	All	All
Operating System	Juniper	Junos	21.3	r1	All	All
Operating System	Juniper	Junos	21.3	r1-s1	All	All
Operating System	Juniper	Junos	21.3	r1-s2	All	All
Operating System	Juniper	Junos	21.3	r2	All	All
Operating System	Juniper	Junos	21.4	-	All	All
Operating System	Juniper	Junos	21.4	r1	All	All
Operating System	Juniper	Junos	21.4	r1-s1	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
Operating System	Juniper	Junos Os Evolved	21.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.2	-	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3	All	All
Operating	Juniper	Junos Os Evolved	21.3	-	All	All

System

Operating System	Juniper	Junos Os Evolved	21.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.4	-	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1	All	All

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:21.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.1:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.1:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.2:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.3:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.3:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.3:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.4:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.4:r1-s1:*:*:*:*:*:*:

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:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.3:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.3:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.4:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.4:r1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@sidfm_jp	Juniper Networks Junos OS の RPD の処理にサービスを妨害される問題 (CVE-2022-22213) [42784] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2022-07-15 07:00:10
@CVEreport	CVE-2022-22213 : A vulnerability in Handling of Undefined Values in the routing protocol daemon RPD process of Ju… twitter.com/i/web/status/1…	2022-07-20 14:21:11
/r/netcve	CVE-2022-22213	2022-07-20 15:38:46

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report