



CVE-2021-31353

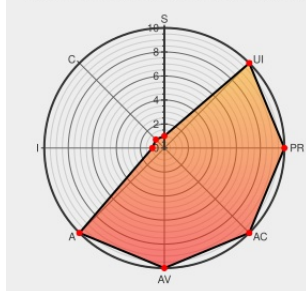
Published on: 10/19/2021 12:00:00 AM UTC

Last Modified on: 10/25/2021 09:41:00 PM UTC

CVE-2021-31353 - advisory for JSA11218

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

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



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

An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an attacker to inject a specific BGP update, causing the routing protocol daemon (RPD) to crash and restart, leading to a Denial of Service (DoS). Continued receipt and processing of the BGP update will create a sustained

Denial of Service (DoS) condition. This issue affects very specific versions of Juniper Networks Junos OS: 19.3R3-S2; 19.4R3-S3; 20.2 versions 20.2R2-S3 and later, prior to 20.2R3-S2; 20.3 versions 20.3R2 and later, prior to 20.3R3; 20.4 versions 20.4R2 and later, prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS 20.1 is not affected by this issue. This issue also affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO, 20.4R3-EVO; 21.1-EVO versions prior to 21.1R2-EVO; 21.2-EVO versions prior to 21.2R2-EVO.

CVE-2021-31353 has been assigned by [J sirt@juniper.net](#) to track the vulnerability - currently rated as **HIGH** severity.

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

Vulnerability Patch/Work Around

This issue can be mitigated in two ways: 1) ensure that TTL propagation is either enabled or disabled in both places below: protocols mpls no-propagate-ttl routing-instance no-vrf-propagate-ttl 2) Disable multipath: routing-instance routing-options multipath

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: 5 - MEDIUM						
Access Vector	Access Complexity	Authentication				
NETWORK	LOW	NONE				
Confidentiality Impact	Integrity Impact	Availability Impact				
NONE	NONE	PARTIAL				
CVE References						
Description	Tags	Link				
2021-10 Security Bulletin: Junos OS and Junos OS Evolved: RPD core upon receipt of specific BGP update (CVE-2021-31353) - Juniper Networks	kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA11218				
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	19.3	r3-s2	All	All
Operating System	Juniper	Junos	19.4	r3-s3	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	20.3	r2	All	All
Operating System	Juniper	Junos	20.3	r2-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	21.1	r1	All	All
Operating System	Juniper	Junos	21.1	r1-s1	All	All
Operating	Juniper	Junos Os Evolved	20.4	r1	All	All

System						
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	20.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s2	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	21.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	All	All	All	All
cpe:2.3:o:juniper:junos:19.3:r3-s2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:19.4:r3-s3:*:*:*:*:*:						
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:20.3:r2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:20.3:r2-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:21.1:r1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:21.1:r1-s1:*:*:*:*:*:						
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:20.4:r2:*:*:*:*:*:						

cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s2:*****:
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:21.2:r1:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r1-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @softek_jp	Juniper Networks Junos OS の BGP アップデートの処理にサービスを妨害される問題 (CVE-2021-31353) [40239] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2021-10-14 08:30:16
 @CVEreport	CVE-2021-31353 : An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Juno... twitter.com/i/web/status/1...	2021-10-19 18:28:23

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

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