



CVE-2022-22219

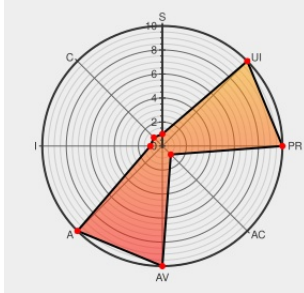
Published on: Not Yet Published

Last Modified on: 10/21/2022 06:12:00 PM UTC

CVE-2022-22219 - advisory for JSA69898

[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:

Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved, an attacker in direct control of a BGP client connected to a route reflector, or via a machine in the middle (MITM) attack, can send a specific EVPN route contained within a BGP Update, triggering

a routing protocol daemon (RPD) crash, leading to a Denial of Service (DoS) condition. Continued receipt and processing of these specific EVPN routes could create a sustained Denial of Service (DoS) condition. This issue only occurs on BGP route reflectors, only within a BGP EVPN multicast environment, and only when one or more BGP clients have 'leave-sync-route-oldstyle' enabled. This issue affects: Juniper Networks Junos OS 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3 version 21.3R1-EVO and later versions prior to 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R3-EVO; 22.2 versions prior to 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.3R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO.

CVE-2022-22219 has been assigned by [J sirt@juniper.net](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Vulnerability Patch/Work Around

Enabling 'leave-sync-route-oldstyle' on the BGP route reflector will mitigate the RPD crash, but BGP sessions may still be torn down if one or more clients have 'leave-sync-route-oldstyle' enabled.

CVSS3 Score: **5.9 - MEDIUM**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK

HIGH

NONE

NONE

Scope

Confidentiality

Integrity

Availability

Impact		Impact		Impact			
UNCHANGED		NONE		NONE		HIGH	
CVE References							
Description		Tags		Link			
evpn EVPN User Guide Juniper Networks TechLibrary		www.juniper.net text/xml		 MISC www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/ref/statement/evpn-edit-routing-instances-protocols.html			
CEC Juniper Community		kb.juniper.net text/html		 CONFIRM kb.juniper.net/JSA69898			
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.							
Related QID Numbers							
43975 Juniper Network Operating System (Junos OS) Denial of Service (DoS) Vulnerability (JSA69898)							
Known Affected Configurations (CPE V2.3)							
Type	Vendor	Product	Version	Update	Edition	Language	
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	21.3	r2-s1	All	All	
Operating System	Juniper	Junos	21.3	r2-s2	All	All	
Operating System	Juniper	Junos	21.3	r3	All	All	
Operating System	Juniper	Junos	21.3	r3-s1	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	21.4	r1-s2	All	All	

System						
Operating System	Juniper	Junos	21.4	r2	All	All
Operating System	Juniper	Junos	21.4	r2-s1	All	All
Operating System	Juniper	Junos	22.1	r1	All	All
Operating System	Juniper	Junos	22.1	r1-s1	All	All
Operating System	Juniper	Junos	22.1	r2	All	All
Operating System	Juniper	Junos	22.1	r2-s2	All	All
Operating System	Juniper	Junos	22.2	r1	All	All
Operating System	Juniper	Junos	22.2	r1-s1	All	All
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	21.3	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	22.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	22.2	r1-s1	All	All
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:21.3:r2-s1:*:*:*:*.*:						
cpe:2.3:o:juniper:junos:21.3:r2-s2:*:*:*:*.*:						

cpe:2.3:o:juniper:junos:21.3:r3:*.***.***:
cpe:2.3:o:juniper:junos:21.3:r3-s1:*.***.***:
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:21.4:r1-s2:*.***.***:
cpe:2.3:o:juniper:junos:21.4:r2:*.***.***:
cpe:2.3:o:juniper:junos:21.4:r2-s1:*.***.***:
cpe:2.3:o:juniper:junos:22.1:r1:*.***.***:
cpe:2.3:o:juniper:junos:22.1:r1-s1:*.***.***:
cpe:2.3:o:juniper:junos:22.1:r2:*.***.***:
cpe:2.3:o:juniper:junos:22.1:r2-s2:*.***.***:
cpe:2.3:o:juniper:junos:22.2:r1:*.***.***:
cpe:2.3:o:juniper:junos:22.2:r1-s1:*.***.***:
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:21.3:r2-s1:*.***.***:
cpe:2.3:o:juniper:junos_os_evolved:21.3:r2-s2:*.***.***:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r1:*.***.***:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r1-s1:*.***.***:
cpe:2.3:o:juniper:junos_os_evolved:22.2:r1:*.***.***:
cpe:2.3:o:juniper:junos_os_evolved:22.2:r1-s1:*.***.***:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔒 @CVEreport	CVE-2022-22219 : Due to the Improper Handling of an Unexpected Data Type in the processing of EVPN routes on Junipe... twitter.com/i/web/status/1...	2022-10-18 02:53:54

© [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](#)