



CVE-2023-22410

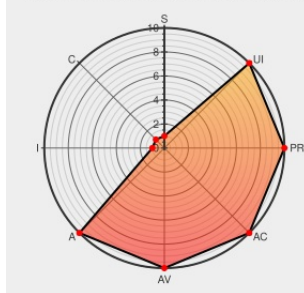
Published on: Not Yet Published

Last Modified on: 01/20/2023 07:58:00 AM UTC

CVE-2023-22410 - advisory for JSA70206

[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:

A Missing Release of Memory after Effective Lifetime vulnerability in the Juniper Networks Junos OS on MX Series platforms with MPC10/MPC11 line cards, allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). Devices are only vulnerable when the Suspicious Control Flow Detection (scfd) feature is enabled. Upon

enabling this specific feature, an attacker sending specific traffic is causing memory to be allocated dynamically and it is not freed. Memory is not freed even after deactivating this feature. Sustained processing of such traffic will eventually lead to an out of memory condition that prevents all services from continuing to function, and requires a manual restart to recover. The FPC memory usage can be monitored using the CLI command "show chassis fpc". On running the above command, the memory of AftDdosScfdFlow can be observed to detect the memory leak. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 20.2R3-S5; 20.3 version 20.3R1 and later versions.

CVE-2023-22410 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.

Affected Vendor/Software: **Juniper Networks - Junos OS** version < 20.2R3-S5

Affected Vendor/Software: **Juniper Networks - Junos OS** version >= 20.3R1

Vulnerability Patch/Work Around

There are no known workarounds for this issue.

CVSS3 Score: **6.5 - MEDIUM**

Attack
Vector

ADJACENT_NETWORK

Attack
Complexity

LOW

Privileges
Required

NONE

User
Interaction

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/JSA70206

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

43956 Juniper Network Operating System (Junos OS) :MX Series Suspicious Control Flow Detection (scfd) Memory Leak Vulnerability (JSA70206)

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	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

System						
Operating System	Juniper	Junos	20.2	r3-s3	All	All
Operating System	Juniper	Junos	20.2	r3-s4	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	20.3	r3-s3	All	All
Operating System	Juniper	Junos	20.3	r3-s4	All	All
Operating System	Juniper	Junos	20.3	r3-s5	All	All
Operating System	Juniper	Junos	20.3	r3-s6	All	All
Hardware  	Juniper	Mx10	-	All	All	All
Hardware  	Juniper	Mx10000	-	All	All	All
Hardware  	Juniper	Mx10003	-	All	All	All
Hardware  	Juniper	Mx10008	-	All	All	All
Hardware  	Juniper	Mx10016	-	All	All	All
Hardware  	Juniper	Mx104	-	All	All	All
Hardware  	Juniper	Mx150	-	All	All	All
Hardware  	Juniper	Mx2008	-	All	All	All
Hardware  	Juniper	Mx2010	-	All	All	All
Hardware  	Juniper	Mx2020	-	All	All	All
Hardware  	Juniper	Mx2024	-	All	All	All

Hardware		Juniper	Mx204	-	All	All	All
Hardware		Juniper	Mx240	-	All	All	All
Hardware		Juniper	Mx40	-	All	All	All
Hardware		Juniper	Mx480	-	All	All	All
Hardware		Juniper	Mx5	-	All	All	All
Hardware		Juniper	Mx80	-	All	All	All
Hardware		Juniper	Mx960	-	All	All	All
cpe:2.3:o:juniper:junos:*.*.*.*.*.*:							
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:20.2:r3-s3:.*.*.*.*.*:							
cpe:2.3:o:juniper:junos:20.2:r3-s4:.*.*.*.*.*:							
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:h:juniper:mx960:-:*:*:*:*:*:*:
```

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](#)