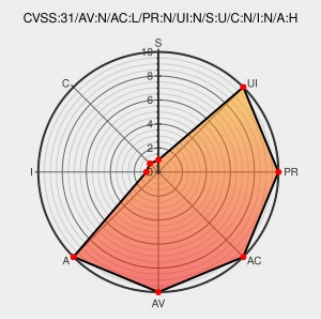
CVE-2023-22410

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



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	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	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/JSA70206

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

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	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:o:juniper:junos:20.3:r3-s1:*:*:*:*:*:*:*

cpe:2.3:o:juniper:junos:20.3:r3-s2:*:*:*:*:*:*:*

cpe:2.3:o:juniper:junos:20.3:r3-s3:*:*:*:*:*:*:*

cpe:2.3:o:juniper:junos:20.3:r3-s4:*:*:*:*:*:*:*

cpe:2.3:o:juniper:junos:20.3:r3-s5:*:*:*:*:*:*:*

cpe:2.3:o:juniper:junos:20.3:r3-s6:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx10:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx10000:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx10003:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx10008:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx10016:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx104:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx150:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx2008:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx2010:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx2020:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx204:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx240:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx40:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx480:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx5:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx80:-:*:*:*:*:*:*:*

cpe:2.3:h:juniper:mx960:-:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-22410 : A Missing Release of Memory after Effective Lifetime vulnerability in the Juniper Networks Junos O… twitter.com/i/web/status/1…	2023-01-13 00:00:49

← Previous ID

Next ID→

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