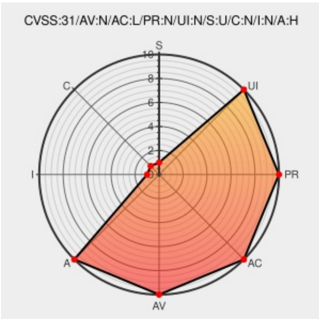
CVE-2021-31351

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

Last Modified on: 10/25/2021 09:27:00 PM UTC

CVE-2021-31351 - advisory for JSA11216

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



Certain versions of Junos from Juniper contain the following vulnerability:

An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240;

CVE-2021-31351 has been assigned by 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

There are no viable workarounds for this issue.

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	Access	Authentication

Vector	Complexity	
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
2021-10 Security Bulletin: Junos OS: MX Series: Receipt of specific packet on MS-MPC/MS-MIC causes line card reset (CVE-2021-31351) - Juniper Networks	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA11216

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

43895 Juniper Network Operating System (Junos OS) :MX Series Denial of Service (DoS) (Line Card Reset) Vulnerability (JSA1121)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	17.3	r3-s11	All	All
Operating System	Juniper	Junos	17.4	r2-s13	All	All
Operating System	Juniper	Junos	17.4	r3	All	All
Operating System	Juniper	Junos	17.4	r3-s1	All	All
Operating System	Juniper	Junos	17.4	r3-s2	All	All
Operating System	Juniper	Junos	17.4	r3-s3	All	All
Operating System	Juniper	Junos	17.4	r3-s4	All	All
Operating System	Juniper	Junos	18.1	r3-s12	All	All
Operating System	Juniper	Junos	18.2	r2-s8	All	All
Operating System	Juniper	Junos	18.2	r3-s7	All	All
Operating System	Juniper	Junos	18.2	r3-s8	All	All
Operating System	Juniper	Junos	18.3	r3-s4	All	All

Operating System	Juniper	Junos	18.4	r3-s7	All	All
Operating System	Juniper	Junos	19.1	r3-s4	All	All
Operating System	Juniper	Junos	19.1	r3-s5	All	All
Operating System	Juniper	Junos	19.2	r1-s6	All	All
Operating System	Juniper	Junos	19.3	r3-s2	All	All
Operating System	Juniper	Junos	19.4	r2-s4	All	All
Operating System	Juniper	Junos	19.4	r2-s5	All	All
Operating System	Juniper	Junos	19.4	r3-s2	All	All
Operating System	Juniper	Junos	20.1	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	20.3	r2	All	All
Operating System	Juniper	Junos	20.3	r2-s1	All	All
Operating System	Juniper	Junos	20.4	r1	All	All
Operating System	Juniper	Junos	20.4	r1-s1	All	All
Operating System	Juniper	Junos	20.4	r2	All	All
Operating System	Juniper	Junos	21.1	r1	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	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:17.3:r3-s11:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.4:r2-s13:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.4:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.4:r3-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.4:r3-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.4:r3-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.4:r3-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.1:r3-s12:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2:r2-s8:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2:r3-s7:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2:r3-s8:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.3:r3-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r3-s7:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r3-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r3-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r3-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r2-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r2-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r3-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1: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:20.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.3:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.4:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.4:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:21.1:r1:*:*:*:*:*:*:

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)
@softek_jp	Juniper Networks MX シリーズの Junos OS にサービスを妨害される問題 (CVE-2021-31351) [40232] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-10-14 08:00:14
@management_sun	IT Risk:Juniper Networks. Junos OS on MX Seriesに複数の脆弱性 悪意ある攻撃者による特定のパケット送出、リセット、Dosによるサービス拒否に至る可能性 CVE-2021-31351 C… twitter.com/i/web/status/1…	2021-10-14 23:12:44
@CVEreport	CVE-2021-31351 : An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC… twitter.com/i/web/status/1…	2021-10-19 18:23:02

← Previous ID

Next ID→