

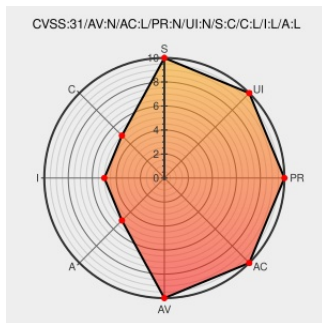


CVE-2020-1660

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:46 PM UTC

CVE-2020-1660 - advisory for JSA11054

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

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

When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets processed by the Multiservices PIC Management Daemon (mspmmand) process, responsible for managing "URL Filtering service", may crash, causing the Services PIC to restart.

While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC completes its boot process. This vulnerability might allow an attacker to cause an extended Denial of Service (DoS) attack against the device and to cause clients to be vulnerable to DNS based attacks by malicious DNS servers when they send DNS requests through the device. As a result, devices which were once protected by the DNS Filtering service are no longer protected and at risk of exploitation. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect Juniper Networks Junos OS 17.4, 18.1, and 18.2.

CVE-2020-1660 has been assigned by [J](#) sirt@juniper.net to track the vulnerability - currently rated as **CRITICAL** 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: **9.9 - CRITICAL**

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

impact		impact		impact	
CHANGED		LOW		LOW	
				HIGH	
CVSS2 Score: 6.8 - MEDIUM					
Access Vector		Access Complexity		Authentication	
NETWORK		MEDIUM		NONE	
Confidentiality Impact		Integrity Impact		Availability Impact	
PARTIAL		PARTIAL		PARTIAL	

CVE References			
Description		Tags	Link
2020-10 Security Bulletin: Junos OS: MX Series: Receipt of specific packets can cause services card to restart when DNS filtering is configured. (CVE-2020-1660) - Juniper Networks		Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA11054
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	
43826 Juniper Junos OS:MX Series Denial of Service (DNS Filtering)vulnerability(JSA11054)	

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	17.3	-	All	All
Operating System	Juniper	Junos	17.3	r1-s1	All	All
Operating System	Juniper	Junos	17.3	r2	All	All
Operating System	Juniper	Junos	17.3	r2-s1	All	All
Operating System	Juniper	Junos	17.3	r2-s2	All	All
Operating System	Juniper	Junos	17.3	r2-s3	All	All
Operating System	Juniper	Junos	17.3	r2-s4	All	All
Operating System	Juniper	Junos	17.3	r2-s5	All	All
Operating System	Juniper	Junos	17.3	r3	-	All
Operating System	Juniper	Junos	17.3	r3-s1	All	All

Operating System	Juniper	Junos	18.4	r2	All	All
Operating System	Juniper	Junos	18.4	r2-s1	All	All
Operating System	Juniper	Junos	18.4	r2-s2	All	All
Operating System	Juniper	Junos	18.4	r2-s3	All	All
Operating System	Juniper	Junos	18.4	r2-s4	All	All
Operating System	Juniper	Junos	19.1	-	All	All
Operating System	Juniper	Junos	19.1	r1	All	All
Operating System	Juniper	Junos	19.1	r1-s1	All	All
Operating System	Juniper	Junos	19.1	r1-s2	All	All
Operating System	Juniper	Junos	19.1	r1-s3	All	All
Operating System	Juniper	Junos	19.1	r1-s4	All	All
Operating System	Juniper	Junos	19.1	r2	All	All
Operating System	Juniper	Junos	19.1	r2-s1	All	All
Operating System	Juniper	Junos	19.2	-	All	All
Operating System	Juniper	Junos	19.2	r1	All	All
Operating System	Juniper	Junos	19.2	r1-s1	All	All
Operating System	Juniper	Junos	19.2	r1-s2	All	All
Operating System	Juniper	Junos	19.2	r1-s3	All	All
Operating System	Juniper	Junos	19.3	-	All	All
Operating System	Juniper	Junos	19.3	r1	All	All
Operating System	Juniper	Junos	19.3	r1-s1	All	All
Operating System	Juniper	Junos	19.3	r2	All	All
Operating System	Juniper	Junos	19.3	r2-s1	All	All

Operating System	Juniper	Junos	19.3	r2-s2	All	All
Operating System	Juniper	Junos	17.3	-	All	All
Operating System	Juniper	Junos	17.3	r1-s1	All	All
Operating System	Juniper	Junos	17.3	r2	All	All
Operating System	Juniper	Junos	17.3	r2-s1	All	All
Operating System	Juniper	Junos	17.3	r2-s2	All	All
Operating System	Juniper	Junos	17.3	r2-s3	All	All
Operating System	Juniper	Junos	17.3	r2-s4	All	All
Operating System	Juniper	Junos	17.3	r2-s5	All	All
Operating System	Juniper	Junos	17.3	r3	-	All
Operating System	Juniper	Junos	17.3	r3-s1	All	All
Operating System	Juniper	Junos	17.3	r3-s2	All	All
Operating System	Juniper	Junos	17.3	r3-s3	All	All
Operating System	Juniper	Junos	17.3	r3-s4	All	All
Operating System	Juniper	Junos	17.3	r3-s7	All	All
Operating System	Juniper	Junos	18.3	-	All	All
Operating System	Juniper	Junos	18.3	r1	All	All
Operating System	Juniper	Junos	18.3	r1-s1	All	All
Operating System	Juniper	Junos	18.3	r1-s2	All	All
Operating System	Juniper	Junos	18.3	r1-s3	All	All
Operating System	Juniper	Junos	18.3	r1-s5	All	All
Operating System	Juniper	Junos	18.3	r1-s6	All	All
Operating System	Juniper	Junos	18.3	r2	All	All

Operating System	Juniper	Junos	18.3	r2-s1	All	All
Operating System	Juniper	Junos	18.3	r2-s2	All	All
Operating System	Juniper	Junos	18.3	r2-s3	All	All
Operating System	Juniper	Junos	18.3	r3	All	All
Operating System	Juniper	Junos	18.4	-	All	All
Operating System	Juniper	Junos	18.4	r1	All	All
Operating System	Juniper	Junos	18.4	r1-s1	All	All
Operating System	Juniper	Junos	18.4	r1-s2	All	All
Operating System	Juniper	Junos	18.4	r1-s5	All	All
Operating System	Juniper	Junos	18.4	r1-s6	All	All
Operating System	Juniper	Junos	18.4	r2	All	All
Operating System	Juniper	Junos	18.4	r2-s1	All	All
Operating System	Juniper	Junos	18.4	r2-s2	All	All
Operating System	Juniper	Junos	18.4	r2-s3	All	All
Operating System	Juniper	Junos	18.4	r2-s4	All	All
Operating System	Juniper	Junos	19.1	-	All	All
Operating System	Juniper	Junos	19.1	r1	All	All
Operating System	Juniper	Junos	19.1	r1-s1	All	All
Operating System	Juniper	Junos	19.1	r1-s2	All	All
Operating System	Juniper	Junos	19.1	r1-s3	All	All
Operating System	Juniper	Junos	19.1	r1-s4	All	All
Operating System	Juniper	Junos	19.1	r2	All	All
Operating System	Juniper	Junos	19.1	r2-s1	All	All

Operating System	Juniper	Junos	19.2	-	All	All
Operating System	Juniper	Junos	19.2	r1	All	All
Operating System	Juniper	Junos	19.2	r1-s1	All	All
Operating System	Juniper	Junos	19.2	r1-s2	All	All
Operating System	Juniper	Junos	19.2	r1-s3	All	All
Operating System	Juniper	Junos	19.3	-	All	All
Operating System	Juniper	Junos	19.3	r1	All	All
Operating System	Juniper	Junos	19.3	r1-s1	All	All
Operating System	Juniper	Junos	19.3	r2	All	All
Operating System	Juniper	Junos	19.3	r2-s1	All	All
Operating System	Juniper	Junos	19.3	r2-s2	All	All
cpe:2.3:o:juniper:junos:17.3:-:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r1-s1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r2-s1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r2-s2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r2-s3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r2-s4:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r2-s5:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r3:-:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r3-s1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r3-s2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r3-s3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r3-s4:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:17.3:r3-s7:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:18.3:-:*:*:*:*:*:						

cpe:2.3:o:juniper:junos:18.3:r1:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s1:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s2:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s3:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s5:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s6:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2-s1:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2-s2:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2-s3:~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r3:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:-:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s1:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s2:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s5:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s6:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s1:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s2:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s3:~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s4:~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:-:~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1:~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s1:~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s2:~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s3:~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s4:~::~~::~~::

cpe:2.3:o:juniper:junos:19.1:r2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r2-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.2:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.2:r1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.2:r1-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.2:r1-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.2:r1-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.3:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.3:r1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.3:r1-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.3:r2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.3:r2-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.3:r2-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r1-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r2-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r2-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r2-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r2-s4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r2-s5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r3:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r3-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r3-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r3-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r3-s4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:17.3:r3-s7:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1:~::~~::~~::~~::~~::~~::

cpe:2.3:o:juniper:junos:18.3:r1-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r1-s6:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r2-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s6:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r1-s4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:19.1:r2:~::~~::~~::~~::~~::~~::

cpe:2.3:o:juniper:junos:19.1:r2-s1:*****:
cpe:2.3:o:juniper:junos:19.2:-:*****:
cpe:2.3:o:juniper:junos:19.2:r1:*****:
cpe:2.3:o:juniper:junos:19.2:r1-s1:*****:
cpe:2.3:o:juniper:junos:19.2:r1-s2:*****:
cpe:2.3:o:juniper:junos:19.2:r1-s3:*****:
cpe:2.3:o:juniper:junos:19.3:-:*****:
cpe:2.3:o:juniper:junos:19.3:r1:*****:
cpe:2.3:o:juniper:junos:19.3:r1-s1:*****:
cpe:2.3:o:juniper:junos:19.3:r2:*****:
cpe:2.3:o:juniper:junos:19.3:r2-s1:*****:
cpe:2.3:o:juniper:junos:19.3:r2-s2:*****:

No vendor comments have been submitted for this CVE

[← 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](#)