



CVE-2020-1686

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

Last Modified on: 10/19/2022 05:21:00 PM UTC

CVE-2020-1686 - advisory for JSA11083

[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:

On Juniper Networks Junos OS devices, receipt of a malformed IPv6 packet may cause the system to crash and restart (vmcore). This issue can be triggered by a malformed IPv6 packet destined to the Routing Engine. An attacker can repeatedly send the offending packet resulting in an extended Denial of Service condition. Only IPv6 packets can

trigger this issue. IPv4 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS prior to 18.4R1.

CVE-2020-1686 has been assigned by [JJ](#) [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

Standard security best common practices such as limiting packet toward the RE only from trusted networks/host using firewall filter in combination with source address anti-spoofing should be applied to reduce the risk of exposure.

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: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

vector	Complexity	
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
2020-10 Security Bulletin: Junos OS: Kernel crash (vmcore) upon receipt of a malformed IPv6 packet. (CVE-2020-1686) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA11083

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	r3	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	19.2	-	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	19.2	r1-s4	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	19.3	r2-s3	All	All
Operating System	Juniper	Junos	19.4	r1	All	All
Operating System	Juniper	Junos	19.4	r1-s1	All	All
Operating System	Juniper	Junos	19.4	r1-s2	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	r3	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	19.2	-	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	19.2	r1-s4	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	19.3	r2-s3	All	All
Operating System	Juniper	Junos	19.4	r1	All	All
Operating System	Juniper	Junos	19.4	r1-s1	All	All
Operating System	Juniper	Junos	19.4	r1-s2	All	All
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:r3:*:*:*:*:*:						
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:19.2:-:~::~~::~~::~~::~::
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:19.2:r1-s4:~::~~::~~::~~::~::
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:19.3:r2-s3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:19.4:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:19.4:r1-s1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:19.4:r1-s2:~::~~::~~::~~::~::
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:10.4:r1:*:*:*:*:
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:19.2:-:*:*:*:*:
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:19.2:r1-s4:*:*:*:*:
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:19.3:r2-s3:*:*:*:*:
cpe:2.3:o:juniper:junos:19.4:r1:*:*:*:*:
cpe:2.3:o:juniper:junos:19.4:r1-s1:*:*:*:*:
cpe:2.3:o:juniper:junos:19.4:r1-s2:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← 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](#)