



CVE-2020-1683

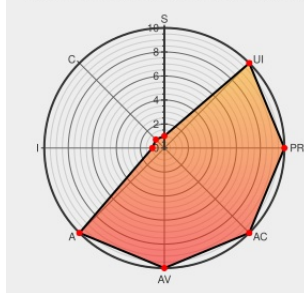
Published on: 10/16/2020 12:00:00 AM UTC

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

CVE-2020-1683 - advisory for JSA11080

[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, a specific SNMP OID poll causes a memory leak which over time leads to a kernel crash (vmcore). Prior to the kernel crash other processes might be impacted, such as failure to establish SSH connection to the device. The administrator can monitor the output of the following command to

check if there is memory leak caused by this issue: `user@device> show system virtual-memory | match "pfe_ipc|kmem"` pfe_ipc 147 5K - 164352 16,32,64,8192 <-- increasing vm.kmem_map_free: 127246336 <-- decreasing pfe_ipc 0 0K - 18598 32,8192 vm.kmem_map_free: 134582272 This issue affects Juniper Networks Junos OS: 17.4R3; 18.1 version 18.1R3-S5 and later versions prior to 18.1R3-S10; 18.2 version 18.2R3 and later versions prior to 18.2R3-S3; 18.2X75 version 18.2X75-D420, 18.2X75-D50 and later versions prior to 18.2X75-D430, 18.2X75-D53, 18.2X75-D60; 18.3 version 18.3R3 and later versions prior to 18.3R3-S2; 18.4 version 18.4R1-S4, 18.4R2 and later versions prior to 18.4R2-S5, 18.4R3-S1; 19.1 version 19.1R2 and later versions prior to 19.1R2-S2, 19.1R3; 19.2 version 19.2R1 and later versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS prior to 17.4R3.

CVE-2020-1683 has been assigned by [J 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

Disable SNMP (disabled by default), utilize edge filtering with source-address validation (uRPF, etc.), access control lists (ACLs), and/or SNMPv3 authentication to limit access to the device only from trusted hosts.

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

CVE References

Description	Tags	Link
2020-10 Security Bulletin: Junos OS: Memory leak leads to kernel crash (vmcore) due to SNMP polling (CVE-2020-1683) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA11080

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	17.4	r3	All	All
Operating System	Juniper	Junos	18.1	r3-s5	All	All
Operating System	Juniper	Junos	18.1	r3-s6	All	All
Operating System	Juniper	Junos	18.1	r3-s7	All	All
Operating System	Juniper	Junos	18.1	r3-s8	All	All
Operating System	Juniper	Junos	18.1	r3-s9	All	All
Operating System	Juniper	Junos	18.2	r3	All	All
Operating System	Juniper	Junos	18.2	r3-s1	All	All
Operating	Juniper	Junos	18.2	r3-s2	All	All

System						
Operating System	Juniper	Junos	18.2x75	-	All	All
Operating System	Juniper	Junos	18.2x75	d12	All	All
Operating System	Juniper	Junos	18.2x75	d20	All	All
Operating System	Juniper	Junos	18.2x75	d30	All	All
Operating System	Juniper	Junos	18.2x75	d40	All	All
Operating System	Juniper	Junos	18.2x75	d411	All	All
Operating System	Juniper	Junos	18.2x75	d51	All	All
Operating System	Juniper	Junos	18.3	r3	All	All
Operating System	Juniper	Junos	18.3	r3-s1	All	All
Operating System	Juniper	Junos	18.4	r1-s4	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	18.4	r3	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	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	Juniper	Junos	19.2	r1-s4	All	All

System						
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	19.3	r2-s4	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	17.4	r3	All	All
Operating System	Juniper	Junos	18.1	r3-s5	All	All
Operating System	Juniper	Junos	18.1	r3-s6	All	All
Operating System	Juniper	Junos	18.1	r3-s7	All	All
Operating System	Juniper	Junos	18.1	r3-s8	All	All
Operating System	Juniper	Junos	18.1	r3-s9	All	All
Operating System	Juniper	Junos	18.2	r3	All	All
Operating System	Juniper	Junos	18.2	r3-s1	All	All
Operating System	Juniper	Junos	18.2	r3-s2	All	All
Operating System	Juniper	Junos	18.2x75	-	All	All
Operating System	Juniper	Junos	18.2x75	d12	All	All
Operating System	Juniper	Junos	18.2x75	d20	All	All

Operating System	Company	Series	Form Factor	Size	Ports	Features
Operating System	Juniper	Junos	18.2x75	d30	All	All
Operating System	Juniper	Junos	18.2x75	d40	All	All
Operating System	Juniper	Junos	18.2x75	d411	All	All
Operating System	Juniper	Junos	18.2x75	d51	All	All
Operating System	Juniper	Junos	18.3	r3	All	All
Operating System	Juniper	Junos	18.3	r3-s1	All	All
Operating System	Juniper	Junos	18.4	r1-s4	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	18.4	r3	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	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	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	19.3	r2-s4	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:17.4:r3:*****:						
cpe:2.3:o:juniper:junos:18.1:r3-s5:*****:						
cpe:2.3:o:juniper:junos:18.1:r3-s6:*****:						
cpe:2.3:o:juniper:junos:18.1:r3-s7:*****:						
cpe:2.3:o:juniper:junos:18.1:r3-s8:*****:						
cpe:2.3:o:juniper:junos:18.1:r3-s9:*****:						
cpe:2.3:o:juniper:junos:18.2:r3:*****:						
cpe:2.3:o:juniper:junos:18.2:r3-s1:*****:						
cpe:2.3:o:juniper:junos:18.2:r3-s2:*****:						
cpe:2.3:o:juniper:junos:18.2x75:-:*****:						
cpe:2.3:o:juniper:junos:18.2x75:d12:*****:						
cpe:2.3:o:juniper:junos:18.2x75:d20:*****:						
cpe:2.3:o:juniper:junos:18.2x75:d30:*****:						
cpe:2.3:o:juniper:junos:18.2x75:d40:*****:						
cpe:2.3:o:juniper:junos:18.2x75:d411:*****:						
cpe:2.3:o:juniper:junos:18.2x75:d51:*****:						
cpe:2.3:o:juniper:junos:18.3:r3:*****:						
cpe:2.3:o:juniper:junos:18.3:r3-s1:*****:						

cpe:2.3:o:juniper:junos:18.4:r1-s4:~::~~::~~::~~::~::
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:18.4:r3:~::~~::~~::~~::~::
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: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:19.3:r2-s4:~::~~::~~::~~::~::
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:17.4:r3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:18.1:r3-s5:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:18.1:r3-s6:~::~~::~~::~~::~::

cpe:2.3:o:juniper:junos:18.1:r3-s7:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.1:r3-s8:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.1:r3-s9:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2:r3:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2:r3-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2:r3-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:-:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:d12:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:d20:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:d30:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:d40:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:d411:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.2x75:d51:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r3:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r3-s1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s4:~::~~::~~::~~::~~::~~::
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:18.4:r3:~::~~::~~::~~::~~::
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: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:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

Next ID→