



# CVE-2020-1640

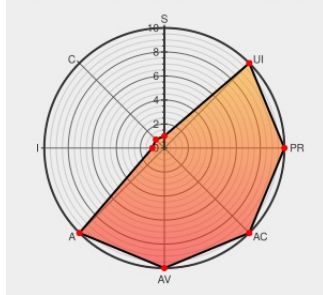
Published on: 07/17/2020 12:00:00 AM UTC

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

## CVE-2020-1640 - advisory for JSA11024

[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:

An improper use of a validation framework when processing incoming genuine BGP packets within Juniper Networks RPD (routing protocols process) daemon allows an attacker to crash RPD thereby causing a Denial of Service (DoS) condition. This framework requires these packets to be passed. By continuously sending any of these types of

formatted genuine packets, an attacker can repeatedly crash the RPD process causing a sustained Denial of Service. Authentication to the BGP peer is not required. This issue can be initiated or propagated through eBGP and iBGP and can impact devices in either modes of use as long as the devices are configured to support the compromised framework and a BGP path is activated or active. This issue affects: Juniper Networks Junos OS 16.1 versions 16.1R7-S6 and later versions prior to 16.1R7-S8; 17.3 versions 17.3R2-S5, 17.3R3-S6 and later versions prior to 17.3R3-S8; 17.4 versions 17.4R2-S7, 17.4R3 and later versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions 18.1R3-S7 and later versions prior to 18.1R3-S10; 18.2 versions 18.2R2-S6, 18.2R3-S2 and later versions prior to 18.2R2-S7, 18.2R3-S5; 18.2X75 versions 18.2X75-D12, 18.2X75-D32, 18.2X75-D33, 18.2X75-D51, 18.2X75-D60, 18.2X75-D411, 18.2X75-D420 and later versions prior to 18.2X75-D32, 18.2X75-D33, 18.2X75-D420, 18.2X75-D52, 18.2X75-D60, 18.2X75-D65, 18.2X75-D70;(\*1) 18.3 versions 18.3R1-S6, 18.3R2-S3, 18.3R3 and later versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions 18.4R1-S5, 18.4R2-S4, 18.4R3 and later versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S3(\*2); 19.1 versions 19.1R1-S3, 19.1R2 and later versions prior to 19.1R1-S5, 19.1R2-S2, 19.1R3-S2; 19.2 versions 19.2R1-S2, 19.2R2 and later versions prior to 19.2R1-S5, 19.2R2, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2, 19.4R3; 20.1 versions prior to 20.1R1-S1, 20.1R2. This issue does not affect Junos OS prior to 16.1R1. This issue affects IPv4 and IPv6 traffic.

CVE-2020-1640 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

There are no available workarounds for this issue.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

#### CVE References

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Tags                                                                                           | Link                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2020-07 Security Bulletin: Junos OS: Receipt of certain genuine BGP packets from any BGP Speaker causes RPD to crash. (CVE-2020-1640) - Juniper Networks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <a href="#">Vendor Advisory</a><br><a href="#">kb.juniper.net</a><br><a href="#">text/html</a> |  <a href="#">MISC</a><br><a href="#">kb.juniper.net/JSA11024</a> |
| 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 <a href="mailto:comment@cve.report">comment@cve.report</a> . |                                                                                                |                                                                                                                                                       |

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type             | Vendor                  | Product               | Version | Update | Edition | Language |
|------------------|-------------------------|-----------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 16.1    | r7-s6  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 16.1    | r7-s7  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.3    | r2-s5  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.3    | r3-s6  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.3    | r3-s7  | All     | All      |

|                  |         |       |         |        |     |     |
|------------------|---------|-------|---------|--------|-----|-----|
| Operating System | Juniper | Junos | 17.4    | r2-s10 | All | All |
| Operating System | Juniper | Junos | 17.4    | r2-s7  | All | All |
| Operating System | Juniper | Junos | 17.4    | r2-s8  | All | All |
| Operating System | Juniper | Junos | 17.4    | r2-s9  | 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 | 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    | r2-s6  | All | All |
| Operating System | Juniper | Junos | 18.2    | r3-s2  | All | All |
| Operating System | Juniper | Junos | 18.2    | r3-s3  | All | All |
| Operating System | Juniper | Junos | 18.2    | r3-s4  | All | All |
| Operating System | Juniper | Junos | 18.2x75 | d12    | 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    | r1-s6  | 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 | 18.3    | r3-s1  | 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-s4  | All | All |

|                  |                         |                       |      |       |     |     |
|------------------|-------------------------|-----------------------|------|-------|-----|-----|
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r3    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r3-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r3-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r1-s3 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r1-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r2    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r2-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r3    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r3-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.2 | r1-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.2 | r1-s3 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.2 | r1-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | -     | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r1-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r2    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r2-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r2-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.4 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.4 | r1-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.1 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 16.1 | r7-s6 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 16.1 | r7-s7 | All | All |

|                  |                         |                       |         |        |     |     |
|------------------|-------------------------|-----------------------|---------|--------|-----|-----|
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.3    | r2-s5  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.3    | r3-s6  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.3    | r3-s7  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.4    | r2-s10 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.4    | r2-s7  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.4    | r2-s8  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.4    | r2-s9  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.4    | r3     | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 17.4    | r3-s1  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.1    | r3-s7  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.1    | r3-s8  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.1    | r3-s9  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2    | r2-s6  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2    | r3-s2  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2    | r3-s3  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2    | r3-s4  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2x75 | d12    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2x75 | d411   | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.2x75 | d51    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.3    | r1-s6  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.3    | r2-s3  | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.3    | r3     | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.3    | r3-s1  | All | All |

|                  |                         |                       |      |       |     |     |
|------------------|-------------------------|-----------------------|------|-------|-----|-----|
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r1-s5 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r1-s6 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r2-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r3    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r3-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 18.4 | r3-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r1-s3 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r1-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r2    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r2-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r3    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.1 | r3-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.2 | r1-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.2 | r1-s3 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.2 | r1-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | -     | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r1-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r2    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r2-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.3 | r2-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.4 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 19.4 | r1-s1 | All | All |

| Operating System                            | Juniper | Junos | 20.1 | r1 | All | All |
|---------------------------------------------|---------|-------|------|----|-----|-----|
| cpe:2.3:o:juniper:junos:16.1:r7-s6:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:16.1:r7-s7:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.3:r2-s5:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.3:r3-s6:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.3:r3-s7:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.4:r2-s10:*****:  |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.4:r2-s7:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.4:r2-s8:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:17.4:r2-s9:*****:   |         |       |      |    |     |     |
| 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: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:r2-s6:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:18.2:r3-s2:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:18.2:r3-s3:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:18.2:r3-s4:*****:   |         |       |      |    |     |     |
| cpe:2.3:o:juniper:junos:18.2x75:d12:*****:  |         |       |      |    |     |     |
| 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:r1-s6:*****:   |         |       |      |    |     |     |
| 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:18.3:r3-s1:*****:   |         |       |      |    |     |     |
| 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-s4:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:18.4:r3:~::~~::~~::~~::~~::~~::     |
| cpe:2.3:o:juniper:junos:18.4:r3-s1:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:18.4:r3-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:19.1:r3:~::~~::~~::~~::~~::~~::     |
| cpe:2.3:o:juniper:junos:19.1:r3-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:19.4:r1:~::~~::~~::~~::~~::~~::     |
| cpe:2.3:o:juniper:junos:19.4:r1-s1:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:20.1:r1:~::~~::~~::~~::~~::~~::     |
| cpe:2.3:o:juniper:junos:16.1:r7-s6:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:16.1:r7-s7:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:17.3:r2-s5:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:17.3:r3-s6:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:17.3:r3-s7:~::~~::~~::~~::~~::~~::  |
| cpe:2.3:o:juniper:junos:17.4:r2-s10:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:17.4:r2-e7:~::~~::~~::~~::~~::~~::  |

```

CPE:2.0.0:juniiper:junos.17.4.12-37 . . . . .

```

```
cpe:2.3:o:juniper:junos:17.4:r2-s8:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:17.4:r2-s9:*:*:*:*:*:
```

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: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:r2-s6:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.2:r3-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.2:r3-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.2:r3-s4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.2x75:d12:*:*:*:*:*:
```

```
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:r1-s6:*:*:*:*:*:
```

```
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:18.3:r3-s1:*:*:*:*:
```

```
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-s4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.4:r3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.4:r3-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:18.4:r3-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:19.1:r3:*:*:*:*:*:    |
| cpe:2.3:o:juniper:junos:19.1:r3-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:19.4:r1:*:*:*:*:*:    |
| cpe:2.3:o:juniper:junos:19.4:r1-s1:*:*:*:*:*: |
| cpe:2.3:o:juniper:junos:20.1:r1:*:*:*:*:*:    |

No vendor comments have been submitted for this CVE

Social Mentions

| Source                                                                                        | Title                                                                                                                                                                                                    | Posted (UTC)        |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @_The_Dust | @farazsth98 hi, i was reading your blog post on CVE-2020-1640 and stubbed something 've really needed to learn from... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-05-22 14:11:32 |

[← 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](#)