



CVE-2019-0064

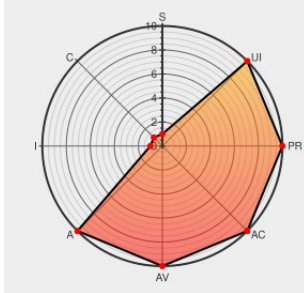
Published on: 10/09/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-0064 - advisory for JSA10963

[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 SRX5000 Series devices, if 'set security zones security-zone <zone> tcp-rst' is configured, the flowd process may crash when a specific TCP packet is received by the device and triggers a new session. The process restarts automatically. However, receipt of a constant stream of these TCP packets may result in an extended Denial of Service (DoS) condition on the device. This issue affects Juniper Networks Junos OS: 18.2R3 on SRX 5000 Series; 18.4R2 on SRX 5000 Series; 19.2R1 on SRX 5000 Series.

CVE-2019-0064 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.

Affected Vendor/Software: **JJ** **Juniper Networks** - **Junos OS** version = **18.2R3**

Affected Vendor/Software: **JJ** **Juniper Networks** - **Junos OS** version = **18.4R2**

Affected Vendor/Software: **JJ** **Juniper Networks** - **Junos OS** version = **19.2R1**

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: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
2019-10 Security Bulletin: Junos OS: SRX5000 Series: flowd process crash due to receipt of specific TCP packet (CVE-2019-0064) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 MISC kb.juniper.net/JSA10963

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	18.2	r3	All	All
Operating System	Juniper	Junos	18.4	r2	All	All
Operating System	Juniper	Junos	19.2	r1	All	All
Operating System	Juniper	Junos	18.2	r3	All	All
Operating System	Juniper	Junos	18.4	r2	All	All
Operating System	Juniper	Junos	19.2	r1	All	All
Hardware  	Juniper	Srx5400	-	All	All	All
Hardware  	Juniper	Srx5400	-	All	All	All
Hardware  	Juniper	Srx5600	-	All	All	All
Hardware  	Juniper	Srx5600	-	All	All	All
Hardware  	Juniper	Srx5800	-	All	All	All
Hardware  	Juniper	Srx5800	-	All	All	All

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

ሰዓቱ 3:00 ሰዓቱ 18:00 ሰዓቱ 18:00 ሰዓቱ 18:00 ሰዓቱ 18:00 ሰዓቱ 18:00

cpe:2.3:o:juniper:junos:10.4:r1:*:*:*:*:
cpe:2.3:o:juniper:junos:19.2:r1:*:*:*:*:
cpe:2.3:o:juniper:junos:18.2:r3:*:*:*:*:
cpe:2.3:o:juniper:junos:18.4:r2:*:*:*:*:
cpe:2.3:o:juniper:junos:19.2:r1:*:*:*:*:
cpe:2.3:h:juniper:srx5400:-:*:*:*:*:
cpe:2.3:h:juniper:srx5400:-:*:*:*:*:
cpe:2.3:h:juniper:srx5600:-:*:*:*:*:
cpe:2.3:h:juniper:srx5600:-:*:*:*:*:
cpe:2.3:h:juniper:srx5800:-:*:*:*:*:
cpe:2.3:h:juniper:srx5800:-:*:*:*:*:

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