



CVE-2021-0235

Published on: 04/22/2021 12:00:00 AM UTC

Last Modified on: 04/27/2021 03:02:00 PM UTC

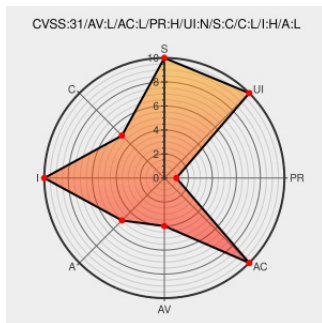
CVE-2021-0235 - advisory for JSA11130

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while

concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1.

CVE-2021-0235 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 viable workarounds for this issue.

CVSS3 Score: 7.3 - HIGH			
Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	HIGH	LOW
CVSS2 Score: 4.6 - MEDIUM			
Access Vector	Access Complexity	Authentication	
LOCAL	LOW	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	PARTIAL	PARTIAL	

CVE References

Description	Tags	Link
2021-04 Security Bulletin: Junos OS: SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series: In a multi-tenant environment, a tenant host administrator may configure logical firewall isolation affecting other tenant networks (CVE-2021-0235) - Juniper Networks	kb.juniper.net text/html	 MISC kb.juniper.net/JSA11130

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

43903 Juniper Network Operating System (JUNOS) SRX Series Incorrect Default Permissions for tenant services Vulnerability (JSA11130)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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-s4	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	r2-s4	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	18.3	r3-s2	All	All
Operating System	Juniper	Junos	18.3	r3-s3	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-s3	All	All
Operating System	Juniper	Junos	18.4	r1-s4	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	r1-s7	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

System						
Operating System	Juniper	Junos	18.4	r2-s4	All	All
Operating System	Juniper	Junos	18.4	r2-s5	All	All
Operating System	Juniper	Junos	18.4	r2-s6	All	All
Operating System	Juniper	Junos	18.4	r3	All	All
Operating System	Juniper	Junos	18.4	r3-s1	All	All
Operating System	Juniper	Junos	18.4	r3-s2	All	All
Operating System	Juniper	Junos	18.4	r3-s3	All	All
Operating System	Juniper	Junos	18.4	r3-s4	All	All
Operating System	Juniper	Junos	18.4	r3-s5	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	r1-s5	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	19.1	r3	All	All
Operating System	Juniper	Junos	19.1	r3-s1	All	All
Operating System	Juniper	Junos	19.1	r3-s2	All	All
Operating System	Juniper	Junos	19.1	r3-s3	All	All
Operating System	Juniper	Junos	19.2	-	All	All
Operating System	Juniper	Junos	19.2	r1	All	All

System						
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	19.2	r1-s5	All	All
Operating System	Juniper	Junos	19.2	r2	All	All
Operating System	Juniper	Junos	19.2	r2-s1	All	All
Operating System	Juniper	Junos	19.2	r3	All	All
Operating System	Juniper	Junos	19.2	r3-s1	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	19.3	r2-s4	All	All
Operating System	Juniper	Junos	19.3	r2-s5	All	All
Operating System	Juniper	Junos	19.3	r3	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	19.4	r2	All	All

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-s4:~::~~::~~::~~::~~::~~::
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:r2-s4:~::~~::~~::~~::~~::~~::
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:18.3:r3-s2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.3:r3-s3:~::~~::~~::~~::~~::~~::
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-s3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r1-s4:~::~~::~~::~~::~~::~~::
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:r1-s7:~::~~::~~::~~::~~::~~::
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:r2-s5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:18.4:r2-s6:~::~~::~~::~~::~~::~~::

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:18.4:r3-s3:*:*:*:*:*:
cpe:2.3:o:juniper:junos:18.4:r3-s4:*:*:*:*:*:
cpe:2.3:o:juniper:junos:18.4:r3-s5:*:*:*:*:*:
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:r1-s5:*:*:*:*:*:
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:19.1:r3-s2:*:*:*:*:*:
cpe:2.3:o:juniper:junos:19.1:r3-s3:*:*:*:*:*:
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:19.2:r1-s5:*:*:*:*:*:
cpe:2.3:o:juniper:junos:19.2:r2:*:*:*:*:*:
cpe:2.3:o:juniper:junos:19.2:r2-s1:*:*:*:*:*:
cpe:2.3:o:juniper:junos:19.2:r3:*:*:*:*:*:

```
cpe:2.3:o:juniper:junos:19.2:r3-s1:*:*:*:*:*:
```

```
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:19.3:r2-s5:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:19.3:r3:*:*:*:*:*:
```

```
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:19.4:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:19.4:r2-s1:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:19.4:r2-s2:*:*:*:*:*:
```

cpe:2.3:o:juniper:junos:19.4:r2-s3:*:*:*:*:*:

```
cpe:2.3:o:juniper:junos:19.4:r3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:19.4:r3-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.1:r1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.1:r1-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.1:r1-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.1:r1-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.1:r1-s4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.2:r1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.2:r1-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.2:r1-s2:*:*:*:*:*:
```

```
cne:2.3:n:iluniner:ilunos:20.2:r1-s3:*.~*.~*.~*.~*.
```

cpe:2.3:o:juniper:junos:20.2:r2:*****:
cpe:2.3:o:juniper:junos:20.3:r1:*****:
cpe:2.3:o:juniper:junos:20.3:r1-s1:*****:
cpe:2.3:h:juniper:srx1500:*****:
cpe:2.3:h:juniper:srx4100:*****:
cpe:2.3:h:juniper:srx4200:*****:
cpe:2.3:h:juniper:srx4600:*****:
cpe:2.3:h:juniper:srx5000:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		