



CVE-2023-44197

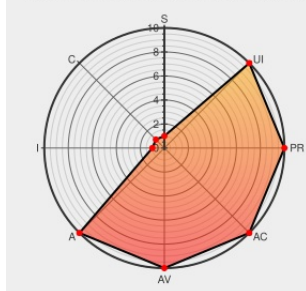
Published on: Not Yet Published

Last Modified on: 10/20/2023 06:38:00 PM UTC

CVE-2023-44197 - advisory for JSA73163

[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 Out-of-Bounds Write vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received

over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R2-S1, 21.4R3-S5. This issue affects Juniper Networks Junos OS Evolved: * All versions prior to 20.4R3-S8-EVO; * 21.1-EVO version 21.1R1-EVO and later versions; * 21.2-EVO versions prior to 21.2R3-S2-EVO; * 21.3-EVO version 21.3R1-EVO and later versions; * 21.4-EVO versions prior to 21.4R2-S1-EVO, 21.4R3-S5-EVO.

CVE-2023-44197 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 known 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

CVE References

Description

Tags

Link

CEC Juniper Community

supportportal.juniper.net

text/html


MISC supportportal.juniper.net/JSA73163

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

All

All

All

All

Operating System

Juniper

Junos

20.4

-

All

All

Operating System

Juniper

Junos

20.4

r1

All

All

Operating System

Juniper

Junos

20.4

r1-s1

All

All

Operating System

Juniper

Junos

20.4

r2

All

All

Operating System

Juniper

Junos

20.4

r2-s1

All

All

Operating System

Juniper

Junos

20.4

r2-s2

All

All

Operating System

Juniper

Junos

20.4

r3

All

All

Operating System

Juniper

Junos

20.4

r3-s1

All

All

Operating System

Juniper

Junos

20.4

r3-s2

All

All

Operating System

Juniper

Junos

20.4

r3-s3

All

All

Operating System

Juniper

Junos

20.4

r3-s4

All

All

Operating System

Juniper

Junos

20.4

r3-s5

All

All

Operating System

Juniper

Junos

20.4

r3-s6

All

All

Operating System

Juniper

Junos

20.4

r3-s7

All

All

Operating System	Juniper	Junos	21.1	r1	All	All
Operating System	Juniper	Junos	21.1	r1-s1	All	All
Operating System	Juniper	Junos	21.1	r2	All	All
Operating System	Juniper	Junos	21.1	r2-s1	All	All
Operating System	Juniper	Junos	21.1	r2-s2	All	All
Operating System	Juniper	Junos	21.1	r3	All	All
Operating System	Juniper	Junos	21.1	r3-s1	All	All
Operating System	Juniper	Junos	21.1	r3-s2	All	All
Operating System	Juniper	Junos	21.1	r3-s3	All	All
Operating System	Juniper	Junos	21.1	r3-s4	All	All
Operating System	Juniper	Junos	21.1	r3-s5	All	All
Operating System	Juniper	Junos	21.2	-	All	All
Operating System	Juniper	Junos	21.2	r1	All	All
Operating System	Juniper	Junos	21.2	r1-s1	All	All
Operating System	Juniper	Junos	21.2	r1-s2	All	All
Operating System	Juniper	Junos	21.2	r2	All	All
Operating System	Juniper	Junos	21.2	r2-s1	All	All
Operating System	Juniper	Junos	21.2	r2-s2	All	All
Operating System	Juniper	Junos	21.2	r3	All	All
Operating System	Juniper	Junos	21.2	r3-s1	All	All
Operating System	Juniper	Junos	21.3	-	All	All
Operating System	Juniper	Junos	21.3	r1	All	All
Operating System	Juniper	Junos	21.3	r1-s1	All	All

System						
Operating System	Juniper	Junos	21.3	r1-s2	All	All
Operating System	Juniper	Junos	21.3	r2	All	All
Operating System	Juniper	Junos	21.3	r2-s1	All	All
Operating System	Juniper	Junos	21.3	r2-s2	All	All
Operating System	Juniper	Junos	21.3	r3	All	All
Operating System	Juniper	Junos	21.3	r3-s1	All	All
Operating System	Juniper	Junos	21.3	r3-s2	All	All
Operating System	Juniper	Junos	21.3	r3-s3	All	All
Operating System	Juniper	Junos	21.3	r3-s4	All	All
Operating System	Juniper	Junos	21.4	-	All	All
Operating System	Juniper	Junos	21.4	r1	All	All
Operating System	Juniper	Junos	21.4	r1-s1	All	All
Operating System	Juniper	Junos	21.4	r1-s2	All	All
Operating System	Juniper	Junos	21.4	r2	All	All
Operating System	Juniper	Junos	21.4	r3	All	All
Operating System	Juniper	Junos	21.4	r3-s1	All	All
Operating System	Juniper	Junos	21.4	r3-s2	All	All
Operating System	Juniper	Junos	21.4	r3-s3	All	All
Operating System	Juniper	Junos	21.4	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	All	All	All	All
Operating System	Juniper	Junos Os Evolved	20.4	-	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s1	All	All

System						
Operating System	Juniper	Junos Os Evolved	20.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s5	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s6	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s7	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	21.2	-	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1	All	All
Operating	Juniper	Junos Os Evolved	21.2	r1-s1	All	All

System						
Operating System	Juniper	Junos Os Evolved	21.2	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	21.4	-	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r3	All	All
Operating	Juniper	Junos Os Evolved	21.4	r3-s1	All	All

[illegible]

cpe:2.3:o:juniper:junos:21.1:r3-s4:*****:
cpe:2.3:o:juniper:junos:21.1:r3-s5:*****:
cpe:2.3:o:juniper:junos:21.2:-:*****:
cpe:2.3:o:juniper:junos:21.2:r1:*****:
cpe:2.3:o:juniper:junos:21.2:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.2:r1-s2:*****:
cpe:2.3:o:juniper:junos:21.2:r2:*****:
cpe:2.3:o:juniper:junos:21.2:r2-s1:*****:
cpe:2.3:o:juniper:junos:21.2:r2-s2:*****:
cpe:2.3:o:juniper:junos:21.2:r3:*****:
cpe:2.3:o:juniper:junos:21.2:r3-s1:*****:
cpe:2.3:o:juniper:junos:21.3:-:*****:
cpe:2.3:o:juniper:junos:21.3:r1:*****:
cpe:2.3:o:juniper:junos:21.3:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.3:r1-s2:*****:
cpe:2.3:o:juniper:junos:21.3:r2:*****:
cpe:2.3:o:juniper:junos:21.3:r2-s1:*****:
cpe:2.3:o:juniper:junos:21.3:r2-s2:*****:
cpe:2.3:o:juniper:junos:21.3:r3:*****:
cpe:2.3:o:juniper:junos:21.3:r3-s1:*****:
cpe:2.3:o:juniper:junos:21.3:r3-s2:*****:
cpe:2.3:o:juniper:junos:21.3:r3-s3:*****:
cpe:2.3:o:juniper:junos:21.3:r3-s4:*****:
cpe:2.3:o:juniper:junos:21.4:-:*****:
cpe:2.3:o:juniper:junos:21.4:r1:*****:
cpe:2.3:o:juniper:junos:21.4:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.4:r1-s2:*****:
cpe:2.3:o:juniper:junos:21.4:r2:*****:
cpe:2.3:o:juniper:junos:21.4:r2-s1:*****:

```

cpe:2.3.0:juniper:junos:21.4.13. . . . .

```

```
cpe:2.3:o:juniper:junos:21.4:r3-s1:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:21.4:r3-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:21.4:r3-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:21.4:r3-s4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:*.:.:.:.:.:.:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:-:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r1:*.~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r1-s1::*:.*:*.*.*
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r1-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r2-s1:::~::~:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r2-s2::*:*:*:*:*
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r2-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r3::*:.*.*.*.*
```

```
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s1:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:20.4:r3-s5:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s6:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s7:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.1:r1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.1:r1-s1:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.1:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3-s1:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.1:r3-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.2:-:*:*:*:*:*
```

```
cpe:2.3:o:juniper:junos os evolved:21.2:r1:::~::~
```

```
cpe:2.3:o:juniper:junos os evolved:21.2:r1-s1.*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.2:r1-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.2:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.2:r2-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.2:r2-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.2:r3::*:*:*:*:*
```

```
cpe:2.3:o:juniper:junos os evolved:21.2:r3-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.3:r1:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.3:r1-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.3:r2:::~::~:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.3:r2-s1.*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.3:r2-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.3:r3:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.3:r3-s1.*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.3:r3-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.3:r3-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.3:r3-s4.*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:-:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r1:::*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r1-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:21.4:r1-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r3:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r3-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r3-s2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos_os_evolved:21.4:r3-s3:*:*:*:*:*:
```

cpe:2.3:o:juniper:junos_os_evolved:21.4:r3-s4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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](#)