

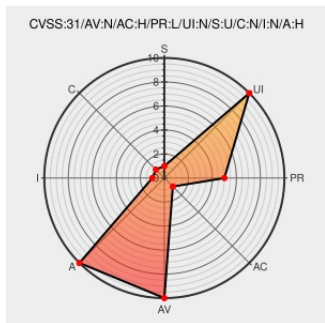


# CVE-2023-44188

Published on: Not Yet Published

Last Modified on: 10/19/2023 04:18:00 PM UTC

## CVE-2023-44188 - advisory for JSA73152

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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

A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in telemetry processing of Juniper Networks Junos OS allows a network-based authenticated attacker to flood the system with multiple telemetry requests, causing the Junos Kernel Debugging Streaming Daemon (jkdsd) process to crash, leading to a Denial of Service (DoS).

Continued receipt and processing of telemetry requests will repeatedly crash the jkdsd process and sustain the Denial of Service (DoS) condition. This issue is seen on all Junos platforms. The crash is triggered when multiple telemetry requests come from different collectors. As the load increases, the Dynamic Rendering Daemon (drend) decides to defer processing and continue later, which results in a timing issue accessing stale memory, causing the jkdsd process to crash and restart. This issue affects: Juniper Networks Junos OS: \* 20.4 versions prior to 20.4R3-S9; \* 21.1 versions 21.1R1 and later; \* 21.2 versions prior to 21.2R3-S6; \* 21.3 versions prior to 21.3R3-S5; \* 21.4 versions prior to 21.4R3-S5; \* 22.1 versions prior to 22.1R3-S4; \* 22.2 versions prior to 22.2R3-S2; \* 22.3 versions prior to 22.3R2-S1, 22.3R3-S1; \* 22.4 versions prior to 22.4R2-S2, 22.4R3; \* 23.1 versions prior to 23.1R2; \* 23.2 versions prior to 23.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.4R1.

CVE-2023-44188 has been assigned by [JJ](#) sirt@juniper.net to track the vulnerability - currently rated as **MEDIUM** severity.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

Affected Vendor/Software: [JJ](#) **Juniper Networks - Junos OS** version **not down converted**

### Vulnerability Patch/Work Around

There are no known workarounds for this issue.

CVSS3 Score: **5.3 - MEDIUM**

Attack

Attack

Privileges

User

| Vector    | Complexity                | Required            | Interaction            |
|-----------|---------------------------|---------------------|------------------------|
| NETWORK   | HIGH                      | LOW                 | NONE                   |
| Scope     | Confidentiality<br>Impact | Integrity<br>Impact | Availability<br>Impact |
| UNCHANGED | NONE                      | NONE                | HIGH                   |

CVE References

| Description           | Tags                                                                   | Link                                                                                                                                      |
|-----------------------|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| CEC Juniper Community | <a href="#">supportportal.juniper.net</a><br><a href="#">text/html</a> |  <a href="#">MISC supportportal.juniper.net/JSA73152</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 [comment@cve.report](mailto: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 | <a href="#">Juniper</a> | <a href="#">Junos</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | -      | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r1     | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r1-s1  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r2     | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r2-s1  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r2-s2  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r3     | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r3-s1  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r3-s2  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r3-s3  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r3-s4  | All     | All      |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 20.4    | r3-s5  | All     | All      |



|                  |                         |                       |      |       |     |     |
|------------------|-------------------------|-----------------------|------|-------|-----|-----|
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.2 | r3    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.2 | r3-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.2 | r3-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.2 | r3-s3 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.2 | r3-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.2 | r3-s5 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | -     | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r1-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r1-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r2    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r2-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r2-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r3    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r3-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r3-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r3-s3 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.3 | r3-s4 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.4 | -     | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.4 | r1    | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.4 | r1-s1 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.4 | r1-s2 | All | All |
| Operating System | <a href="#">Juniper</a> | <a href="#">Junos</a> | 21.4 | r2    | All | All |

|                  |         |       |      |       |     |     |
|------------------|---------|-------|------|-------|-----|-----|
| Operating System | Juniper | Junos | 21.4 | r2-s1 | All | All |
| Operating System | Juniper | Junos | 21.4 | r2-s2 | 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 | 22.1 | r1    | All | All |
| Operating System | Juniper | Junos | 22.1 | r1-s1 | All | All |
| Operating System | Juniper | Junos | 22.1 | r1-s2 | All | All |
| Operating System | Juniper | Junos | 22.1 | r2    | All | All |
| Operating System | Juniper | Junos | 22.1 | r2-s1 | All | All |
| Operating System | Juniper | Junos | 22.1 | r2-s2 | All | All |
| Operating System | Juniper | Junos | 22.1 | r3    | All | All |
| Operating System | Juniper | Junos | 22.1 | r3-s1 | All | All |
| Operating System | Juniper | Junos | 22.1 | r3-s2 | All | All |
| Operating System | Juniper | Junos | 22.1 | r3-s3 | All | All |
| Operating System | Juniper | Junos | 22.2 | r1    | All | All |
| Operating System | Juniper | Junos | 22.2 | r1-s1 | All | All |
| Operating System | Juniper | Junos | 22.2 | r1-s2 | All | All |
| Operating System | Juniper | Junos | 22.2 | r2    | All | All |
| Operating System | Juniper | Junos | 22.2 | r2-s1 | All | All |
| Operating System | Juniper | Junos | 22.2 | r2-s2 | All | All |

|                                               |         |       |      |       |     |     |
|-----------------------------------------------|---------|-------|------|-------|-----|-----|
| Operating System                              | Juniper | Junos | 22.2 | r3    | All | All |
| Operating System                              | Juniper | Junos | 22.2 | r3-s1 | All | All |
| Operating System                              | Juniper | Junos | 22.3 | r1    | All | All |
| Operating System                              | Juniper | Junos | 22.3 | r1-s1 | All | All |
| Operating System                              | Juniper | Junos | 22.3 | r1-s2 | All | All |
| Operating System                              | Juniper | Junos | 22.3 | r2    | All | All |
| Operating System                              | Juniper | Junos | 22.3 | r3    | All | All |
| Operating System                              | Juniper | Junos | 22.4 | r1    | All | All |
| Operating System                              | Juniper | Junos | 22.4 | r1-s1 | All | All |
| Operating System                              | Juniper | Junos | 22.4 | r1-s2 | All | All |
| Operating System                              | Juniper | Junos | 22.4 | r2    | All | All |
| Operating System                              | Juniper | Junos | 22.4 | r2-s1 | All | All |
| Operating System                              | Juniper | Junos | 23.1 | r1    | All | All |
| Operating System                              | Juniper | Junos | 23.2 | r1    | All | All |
| Operating System                              | Juniper | Junos | 23.2 | r1-s1 | All | All |
| cpe:2.3:o:juniper:junos:*.*.*.*.*.*:          |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:-.*.*.*.*.*:     |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r1:*.*.*.*.*:    |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r1-s1:*.*.*.*.*: |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r2:*.*.*.*.*:    |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r2-s1:*.*.*.*.*: |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r2-s2:*.*.*.*.*: |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r3:*.*.*.*.*:    |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r3-s1:*.*.*.*.*: |         |       |      |       |     |     |
| cpe:2.3:o:juniper:junos:20.4:r3-s2:*.*.*.*.*: |         |       |      |       |     |     |

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

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

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

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

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

```
cpe:2.3:o:juniper:junos:20.4:r3-s8:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:21.1:-:*:*:*:*:*:
```

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

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

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

```
cpe:2.3:o:juniper:junos:21.1:r2-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:21.1:r2-s2:*:*:*:*:*:
```

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

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

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

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

```
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:21.2:r3-s2:*:*:*:*:*:
```

[illegible]

|                                           |
|-------------------------------------------|
| cpe:2.3:o:juniper:junos:21.2:r3-s3:*****: |
| cpe:2.3:o:juniper:junos:21.2:r3-s4:*****: |
| cpe:2.3:o:juniper:junos:21.2:r3-s5:*****: |
| 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:o:juniper:junos:21.4:r2-s2:*****: |
| cpe:2.3:o:juniper:junos:21.4:r3:*****:    |
| 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:22.1:r1:*****:    |
| cpe:2.3:o:juniper:junos:22.1:r1-s1:*****: |

|                                                            |
|------------------------------------------------------------|
| cpe:2.3:o:juniper:junos:22.1:r1-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.1:r2:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.1:r2-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.1:r2-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.1:r3:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.1:r3-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.1:r3-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.1:r3-s3:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.2:r1:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.2:r1-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.2:r1-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.2:r2:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.2:r2-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.2:r2-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.2:r3:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.2:r3-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.3:r1:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.3:r1-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.3:r1-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.3:r2:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.3:r3:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.4:r1:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.4:r1-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.4:r1-s2:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:22.4:r2:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:22.4:r2-s1:~::~~::~~::~~::~~::~~:: |
| cpe:2.3:o:juniper:junos:23.1:r1:~::~~::~~::~~::~~::~~::    |
| cpe:2.3:o:juniper:junos:23.2:r1:~::~~::~~::~~::~~::~~::    |

cpe:2.3:o:juniper:junos:23.2:r1-s1:\*.\*\*\*.\*\*\*.\*\*\*:

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](#)