



CVE-2023-36841

Published on: Not Yet Published

Last Modified on: 10/17/2023 04:03:00 PM UTC

CVE-2023-36841 - advisory for JSA73172

[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 Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows a unauthenticated network-based attacker to cause an infinite loop, resulting in a Denial of Service (DoS). An attacker who sends malformed TCP traffic via an interface configured

with PPPoE, causes an infinite loop on the respective PFE. This results in consuming all resources and a manual restart is needed to recover. This issue affects interfaces with PPPoE configured and tcp-mss enabled. This issue affects Juniper Networks Junos OS * All versions prior to 20.4R3-S7; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; * 22.4 versions prior to 22.4R2;

CVE-2023-36841 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/JSA73172
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

44126 Juniper Networks Junos OS Malformed TCP traffic Leads to the Denial of Service (JSA73172)

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	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	21.2	r3-s2	All	All
Operating System	Juniper	Junos	21.2	r3-s3	All	All
Operating System	Juniper	Junos	21.2	r3-s4	All	All
Operating System	Juniper	Junos	21.2	r3-s5	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
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	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	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	22.3	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	r2-s1	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

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:~::~~::~~::
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: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:22.3: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:r2-s1:*:*:*:*:*:
```

```
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:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

© [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](#)