



CVE-2021-31363

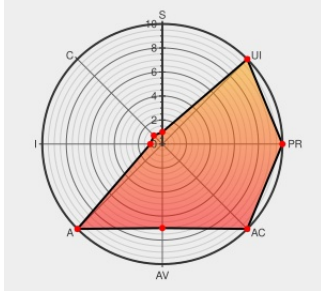
Published on: 10/19/2021 12:00:00 AM UTC

Last Modified on: 10/25/2021 05:14:00 PM UTC

CVE-2021-31363 - advisory for JSA11225

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

CVSS:31/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

In an MPLS P2MP environment a Loop with Unreachable Exit Condition vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause high load on RPD which in turn may lead to routing protocol flaps. If a system with sensor-based-stats enabled

receives a specific LDP FEC this can lead to the above condition. Continued receipt of such an LDP FEC will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 version 19.2R2 and later versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R2-S3-EVO; 20.3 versions prior to 20.3R1-S2-EVO.

CVE-2021-31363 has been assigned by [J SIRT](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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

Vulnerability Patch/Work Around

For Junos OS turn off sensor-based-stats by deleting: [protocols ldp traffic-statistics sensor-based-stats] For Junos OS Evolved mLDP will have to be turned off as sensor-based-stats is the default: [protocols ldp p2mp]

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 3.3 - LOW		
Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
2021-10 Security Bulletin: Junos OS and Junos OS Evolved: Receipt of a specific LDP message will cause a Denial of Service (CVE-2021-31363) - Juniper Networks	kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA11225
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	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	19.2	r3-s2	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-s2	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	r1-s3	All	All
Operating System	Juniper	Junos	19.4	r2-s4	All	All
Operating System	Juniper	Junos	19.4	r3-s2	All	All
Operating System	Juniper	Junos	20.1	r1	All	All
Operating System	Juniper	Junos	20.1	r1-s1	All	All
Operating System	Juniper	Junos	20.1	r1-s2	All	All
Operating System	Juniper	Junos	20.1	r1-s3	All	All
Operating System	Juniper	Junos	20.1	r1-s4	All	All
Operating System	Juniper	Junos	20.1	r2	All	All
Operating System	Juniper	Junos	20.1	r3	All	All
Operating System	Juniper	Junos	20.2	r1	All	All
Operating System	Juniper	Junos	20.2	r1-s1	All	All
Operating System	Juniper	Junos	20.2	r1-s2	All	All
Operating System	Juniper	Junos	20.2	r1-s3	All	All
Operating System	Juniper	Junos	20.2	r2	All	All
Operating System	Juniper	Junos	20.2	r3	All	All

Operating System	Juniper	Junos	20.3	r1	All	All
Operating System	Juniper	Junos	20.3	r1-s1	All	All
Operating System	Juniper	Junos	20.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r1-s1	All	All
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:19.2:r3-s2:*:*:*:*:*:						
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-s2:*:*:*:*:*:
```

```
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:r1-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:19.4:r2-s4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:19.4:r3-s2:*:*:*:*:*:
```

```
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:20.1:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.1:r3:*:*:*:*:*:
```

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

```
cpe:2.3:o:juniper:junos:20.2:r1-s3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.2:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.2:r3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.3:r1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.3:r1-s1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:20.3:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos os evolved:20.1:r1:::~::~:
```

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

```
cpe:2.3:o:juniper:junos_os_evolved:20.1:r2:*:*:*:*:
```

```
cpe:2.3:o:uniper:unos os evolved:20.1:r2-s1::*:.*:.*:.*
```

cpe:2.3:o:juniper:junos_os_evolved:20.1:r2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.2:r1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.2:r1-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.2:r2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.3:r1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.3:r1-s1:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @softek_jp	Juniper Networks Junos OS の RPD の処理にサービスを妨害される問題 (CVE-2021-31363) [40237] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2021-10-14 08:30:15
 @CVEreport	CVE-2021-31363 : In an MPLS P2MP environment a Loop with Unreachable Exit Condition vulnerability in the routing pr... twitter.com/i/web/status/1...	2021-10-19 18:24:25