



CVE-2017-10605

Published on: 07/14/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:28 PM UTC

CVE-2017-10605

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H



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

On all vSRX and SRX Series devices, when the DHCP or DHCP relay is configured, specially crafted packet might cause the flowd process to crash, halting or interrupting traffic from flowing through the device(s). Repeated crashes of the flowd process may constitute an extended denial of service condition for the device(s). If the device is configured

in high-availability, the RG1+ (data-plane) will fail-over to the secondary node. If the device is configured in stand-alone, there will be temporary traffic interruption until the flowd process is restored automatically. Sustained crafted packets may cause the secondary failover node to fail back, or fail completely, potentially halting flowd on both nodes of the cluster or causing flip-flop failovers to occur. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS 12.1X46 prior to 12.1X46-D67 on vSRX or SRX Series; 12.3X48 prior to 12.3X48-D50 on vSRX or SRX Series; 15.1X49 prior to 15.1X49-D91, 15.1X49-D100 on vSRX or SRX Series.

CVE-2017-10605 has been assigned by [JJ](#) sirt@juniper.net to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [JJ](#) **Juniper Networks** - Junos OS version 12.1X46 prior to 12.1X46-D67

Affected Vendor/Software: [JJ](#) **Juniper Networks** - Junos OS version 12.3X48 prior to 12.3X48-D50

Affected Vendor/Software: [JJ](#) **Juniper Networks** - Junos OS version 15.1X49 prior to 15.1X49-D91, 15.1X49-D100

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
2017-07 Security Bulletin: Junos: SRX Series denial of service vulnerability in flowd due to crafted DHCP packet (CVE-2017-10605) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA10789
Juniper Junos DHCP Processing Bug on vSRX and SRX Series Devices Lets Remote Users Cause the Target Service to Crash - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1038891

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	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x46	d10	All	All
Operating System	Juniper	Junos	12.1x46	d15	All	All
Operating System	Juniper	Junos	12.1x46	d20	All	All
Operating System	Juniper	Junos	12.1x46	d25	All	All
Operating System	Juniper	Junos	12.1x46	d30	All	All
Operating System	Juniper	Junos	12.1x46	d35	All	All
Operating System	Juniper	Junos	12.1x46	d40	All	All
Operating System	Juniper	Junos	12.1x46	d45	All	All
Operating	Juniper	Junos	12.1x46	d50	All	All

System						
Operating System	Juniper	Junos	12.1x46	d55	All	All
Operating System	Juniper	Junos	12.1x46	d60	All	All
Operating System	Juniper	Junos	12.1x46	d65	All	All
Operating System	Juniper	Junos	12.3x48	d10	All	All
Operating System	Juniper	Junos	12.3x48	d15	All	All
Operating System	Juniper	Junos	12.3x48	d20	All	All
Operating System	Juniper	Junos	12.3x48	d25	All	All
Operating System	Juniper	Junos	12.3x48	d30	All	All
Operating System	Juniper	Junos	12.3x48	d35	All	All
Operating System	Juniper	Junos	15.1x49	d10	All	All
Operating System	Juniper	Junos	15.1x49	d100	All	All
Operating System	Juniper	Junos	15.1x49	d20	All	All
Operating System	Juniper	Junos	15.1x49	d30	All	All
Operating System	Juniper	Junos	15.1x49	d35	All	All
Operating System	Juniper	Junos	15.1x49	d40	All	All
Operating System	Juniper	Junos	15.1x49	d45	All	All
Operating System	Juniper	Junos	15.1x49	d50	All	All
Operating System	Juniper	Junos	15.1x49	d55	All	All
Operating System	Juniper	Junos	15.1x49	d60	All	All
Operating System	Juniper	Junos	15.1x49	d65	All	All
Operating System	Juniper	Junos	15.1x49	d70	All	All
Operating System	Juniper	Junos	15.1x49	d75	All	All
Operating	Juniper	Junos	15.1x49	d80	All	All

System						
Operating System	Juniper	Junos	15.1x49	d90	All	All
Operating System	Juniper	Junos	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x46	d10	All	All
Operating System	Juniper	Junos	12.1x46	d15	All	All
Operating System	Juniper	Junos	12.1x46	d20	All	All
Operating System	Juniper	Junos	12.1x46	d25	All	All
Operating System	Juniper	Junos	12.1x46	d30	All	All
Operating System	Juniper	Junos	12.1x46	d35	All	All
Operating System	Juniper	Junos	12.1x46	d40	All	All
Operating System	Juniper	Junos	12.1x46	d45	All	All
Operating System	Juniper	Junos	12.1x46	d50	All	All
Operating System	Juniper	Junos	12.1x46	d55	All	All
Operating System	Juniper	Junos	12.1x46	d60	All	All
Operating System	Juniper	Junos	12.1x46	d65	All	All
Operating System	Juniper	Junos	12.3x48	d10	All	All
Operating System	Juniper	Junos	12.3x48	d15	All	All
Operating System	Juniper	Junos	12.3x48	d20	All	All
Operating System	Juniper	Junos	12.3x48	d25	All	All
Operating System	Juniper	Junos	12.3x48	d30	All	All
Operating System	Juniper	Junos	12.3x48	d35	All	All
Operating System	Juniper	Junos	15.1x49	d10	All	All
Operating System	Juniper	Junos	15.1x49	d100	All	All
Operating	Juniper	Junos	15.1x49	d20	All	All

System						
Operating System	Juniper	Junos	15.1x49	d30	All	All
Operating System	Juniper	Junos	15.1x49	d35	All	All
Operating System	Juniper	Junos	15.1x49	d40	All	All
Operating System	Juniper	Junos	15.1x49	d45	All	All
Operating System	Juniper	Junos	15.1x49	d50	All	All
Operating System	Juniper	Junos	15.1x49	d55	All	All
Operating System	Juniper	Junos	15.1x49	d60	All	All
Operating System	Juniper	Junos	15.1x49	d65	All	All
Operating System	Juniper	Junos	15.1x49	d70	All	All
Operating System	Juniper	Junos	15.1x49	d75	All	All
Operating System	Juniper	Junos	15.1x49	d80	All	All
Operating System	Juniper	Junos	15.1x49	d90	All	All
Hardware 	Juniper	Srx100	-	All	All	All
Hardware 	Juniper	Srx100	-	All	All	All
Hardware 	Juniper	Srx110	-	All	All	All
Hardware 	Juniper	Srx110	-	All	All	All
Hardware 	Juniper	Srx1400	-	All	All	All
Hardware 	Juniper	Srx1400	-	All	All	All
Hardware 	Juniper	Srx210	-	All	All	All
Hardware 	Juniper	Srx210	-	All	All	All
Hardware 	Juniper	Srx220	-	All	All	All
Hardware 	Juniper	Srx220	-	All	All	All
Hardware 	Juniper	Srx240	-	All	All	All
Hardware 	Juniper	Srx240	-	All	All	All
Hardware 	Juniper	Srx3400	-	All	All	All
Hardware 	Juniper	Srx3400	-	All	All	All

УРЕ.2.0.0.1011001.101103.12.0X70.000.

```
cpe:2.3:o:juniper:junos:12.3x48:d35:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d10:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d100:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d20:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d30:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d35:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d40:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d45:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d50:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d55:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d60:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d65:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d70:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d75:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d80:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d90:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x46:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x46:d10:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d15:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d20::*:*:*:*:*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d25:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x46:d30:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d35:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x46:d40:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x46:d45:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d50:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d55:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d60:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:12.1x46:d65:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.3x48:d10:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.3x48:d15:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.3x48:d20:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.3x48:d25:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.3x48:d30:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.3x48:d35:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d10:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d100:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d20:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d30:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d35:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d40:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d45:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d50:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d55:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d60:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d65:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d70:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d75:*.~*~*~*~*~*
```

```
cpe:2.3:o:juniper:junos:15.1x49:d80:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1x49:d90:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx100:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx100:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx110:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx110:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx1400:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx1400:-:*:*:*:*:*:*:
```

cpe:2.3:h:juniper:srx210:-:*****:
cpe:2.3:h:juniper:srx210:-:*****:
cpe:2.3:h:juniper:srx220:-:*****:
cpe:2.3:h:juniper:srx220:-:*****:
cpe:2.3:h:juniper:srx240:-:*****:
cpe:2.3:h:juniper:srx240:-:*****:
cpe:2.3:h:juniper:srx3400:-:*****:
cpe:2.3:h:juniper:srx3400:-:*****:
cpe:2.3:h:juniper:srx3600:-:*****:
cpe:2.3:h:juniper:srx3600:-:*****:
cpe:2.3:h:juniper:srx5400:-:*****:
cpe:2.3:h:juniper:srx5400:-:*****:
cpe:2.3:h:juniper:srx550:-:*****:
cpe:2.3:h:juniper:srx550:-:*****:
cpe:2.3:h:juniper:srx5600:-:*****:
cpe:2.3:h:juniper:srx5600:-:*****:
cpe:2.3:h:juniper:srx5800:-:*****:
cpe:2.3:h:juniper:srx5800:-:*****:
cpe:2.3:h:juniper:srx650:-:*****:
cpe:2.3:h:juniper:srx650:-:*****:

[← 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