

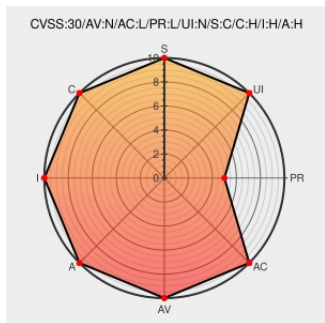


CVE-2017-2349

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

Last Modified on: 03/23/2021 11:26:52 PM UTC

CVE-2017-2349

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

Certain versions of **Junos** from **Juniper** contain the following vulnerability:

A command injection vulnerability in the IDP feature of Juniper Networks Junos OS on SRX series devices potentially allows a user with login access to the device to execute shell commands and elevate privileges. Affected releases are Juniper Networks Junos OS 12.1X44 prior to 12.1X44-D60; 12.1X46 prior to 12.1X46-D50; 12.1X47 prior to 12.1X47-D30, 12.1X47-D35; 12.3X48 prior to 12.3X48-D20, 12.3X48-D30; 15.1X49 prior to 15.1X49-D20, 15.1X49-D30.

CVE-2017-2349 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 **12.1X44** prior to **12.1X44-D60**

Affected Vendor/Software: **JJ** **Juniper Networks - Junos OS** version **12.1X46** prior to **12.1X46-D50**

Affected Vendor/Software: **JJ** **Juniper Networks - Junos OS** version **12.1X47** prior to **12.1X47-D30, 12.1X47-D35**

Affected Vendor/Software: **JJ** **Juniper Networks - Junos OS** version **12.3X48** prior to **12.3X48-D20, 12.3X48-D30**

Affected Vendor/Software: **JJ** **Juniper Networks - Junos OS** version **15.1X49** prior to **15.1X49-D20, 15.1X49-D30**

Vulnerability Patch/Work Around

Use access lists or firewall filters to limit access to the router's CLI only from trusted hosts. Restrict access to the CLI to only highly trusted administrators.

CVSS3 Score: **8.8 - HIGH**

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

UNCHANGEDHIGHHIGHHIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
2017-07 Security Bulletin: SRX Series: Command injection vulnerability in SRX IDP feature. (CVE-2017-2349) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA10801
Juniper Junos on SRX Series Devices Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1038898

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	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x44	d10	All	All
Operating System	Juniper	Junos	12.1x44	d15	All	All
Operating System	Juniper	Junos	12.1x44	d20	All	All
Operating System	Juniper	Junos	12.1x44	d25	All	All
Operating System	Juniper	Junos	12.1x44	d30	All	All
Operating System	Juniper	Junos	12.1x44	d35	All	All
Operating System	Juniper	Junos	12.1x44	d40	All	All
Operating System	Juniper	Junos	12.1x44	d45	All	All

Operating System	Juniper	Junos	12.1x44	d50	All	All
Operating System	Juniper	Junos	12.1x44	d55	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	12.1x47	All	All	All
Operating System	Juniper	Junos	12.1x47	d10	All	All
Operating System	Juniper	Junos	12.1x47	d15	All	All
Operating System	Juniper	Junos	12.1x47	d20	All	All
Operating System	Juniper	Junos	12.1x47	d25	All	All
Operating System	Juniper	Junos	12.1x47	d35	All	All
Operating System	Juniper	Junos	12.3x48	All	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	d30	All	All

Operating System	Juniper	Junos	15.1x49	d10	All	All
Operating System	Juniper	Junos	15.1x49	d15	All	All
Operating System	Juniper	Junos	15.1x49	d30	All	All
Operating System	Juniper	Junos	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x44	d10	All	All
Operating System	Juniper	Junos	12.1x44	d15	All	All
Operating System	Juniper	Junos	12.1x44	d20	All	All
Operating System	Juniper	Junos	12.1x44	d25	All	All
Operating System	Juniper	Junos	12.1x44	d30	All	All
Operating System	Juniper	Junos	12.1x44	d35	All	All
Operating System	Juniper	Junos	12.1x44	d40	All	All
Operating System	Juniper	Junos	12.1x44	d45	All	All
Operating System	Juniper	Junos	12.1x44	d50	All	All
Operating System	Juniper	Junos	12.1x44	d55	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

cpe:2.3:o:juniper:junos:12.1x44:d50:*****:
cpe:2.3:o:juniper:junos:12.1x44:d55:*****:
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:12.1x47:*****:
cpe:2.3:o:juniper:junos:12.1x47:d10:*****:
cpe:2.3:o:juniper:junos:12.1x47:d15:*****:
cpe:2.3:o:juniper:junos:12.1x47:d20:*****:
cpe:2.3:o:juniper:junos:12.1x47:d25:*****:
cpe:2.3:o:juniper:junos:12.1x47:d35:*****:
cpe:2.3:o:juniper:junos:12.3x48:*****:
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:d30:*****:
cpe:2.3:o:juniper:junos:15.1x49:d10:*****:
cpe:2.3:o:juniper:junos:15.1x49:d15:*****:
cpe:2.3:o:juniper:junos:15.1x49:d30:*****:
cpe:2.3:o:juniper:junos:12.1x44:*****:
cpe:2.3:o:juniper:junos:12.1x44:d10:*****:
cpe:2.3:o:juniper:junos:12.1x44:d15:*****:

```
cpe:2.3:o:juniper:junos:12.1x44:d20:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d25:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d30:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d35:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d40:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d45:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d50:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x44:d55:*:*:*:*:*:
```

```
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:12.1x47:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x47:d10:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x47:d15:*.:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x47:d20:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x47:d25:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:12.1x47:d35:*:*:*:*:*:
```

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

```
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:d30:~::~~::~~::
cpe:2.3:o:juniper:junos:15.1x49:d10:~::~~::~~::
cpe:2.3:o:juniper:junos:15.1x49:d15:~::~~::~~::
cpe:2.3:o:juniper:junos:15.1x49:d30:~::~~::~~::

← 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](#)