

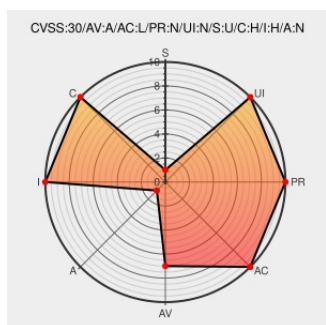


CVE-2017-2342

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

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

CVE-2017-2342

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

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

MACsec feature on Juniper Networks Junos OS 15.1X49 prior to 15.1X49-D100 on SRX300 series does not report errors when a secure link can not be established. It falls back to an unencrypted link. This can happen when MACsec is configured on ports that are not capable of MACsec or when a secure link can not be established. This can

mislead customers into believing that a link is secure. On SRX 300 series devices, prior to 15.1X49-D100, MACsec was only supported on control and fabric ports of SRX340 and SRX345 devices. SRX300 and SRX320 did not have any MACsec capable ports. Configuring MACsec on ports that were not MACsec capable would have resulted in this issue. Affected releases are Juniper Networks Junos OS 15.1X49 prior to 15.1X49-D100 on SRX300 series.

CVE-2017-2342 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 **15.1X49** prior to **15.1X49-D100**

Vulnerability Patch/Work Around

There are no viable workarounds for this issue. It is good security practice to limit the exploitable attack surface of critical infrastructure networking equipment. Use access lists or firewall filters to limit access to the device from trusted, administrative networks or hosts.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Juniper Junos SRX300 Series MACsec Non-Secure Fallback Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1038890
2017-07 Security Bulletin: SRX Series: MACsec failure to report errors (CVE-2017-2342) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA10790

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	15.1x49	d10	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 System	Juniper	Junos	15.1x49	d80	All	All
Operating System	Juniper	Junos	15.1x49	d90	All	All
Operating System	Juniper	Junos	15.1x49	d10	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 System	Juniper	Junos	15.1x49	d80	All	All
Operating System	Juniper	Junos	15.1x49	d90	All	All
Hardware 🇵🇪🔗	Juniper	Srx300	-	All	All	All
Hardware 🇵🇪🔗	Juniper	Srx300	-	All	All	All
cpe:2.3:o:juniper:junos:15.1x49:d10:*:*:*:*:*:						
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:15.1x49:d10:~::~~::~~::~~::
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:srx300:~::~~::~~::~~::
cpe:2.3:h:juniper:srx300:~::~~::~~::~~::

Discovery Credit

Array

© [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](#)