



CVE-2015-3007

Published on: 07/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:08 PM UTC

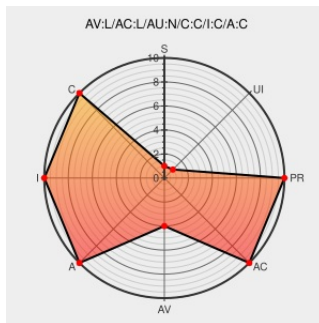
CVE-2015-3007

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The Juniper SRX Series services gateways with Junos OS 12.1X46 before 12.1X46-D35, 12.1X47 before 12.1X47-D25, and 12.3X48 before 12.3X48-D15 do not properly implement the "set system ports console insecure" feature, which allows physically proximate attackers to gain administrative privileges by leveraging access to the console

port.

CVE-2015-3007 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Juniper Junos SRX Series Console Port Access Control Flaw Lets Local Users Gain Root Privileges - SecurityTracker	www.securitytracker.com text/html	SECTrack 1032841
Juniper Networks - 2015-07 Security Bulletin: Junos: SRX 'set system ports console insecure' not functioning as expected (CVE-2015-3007) - Knowledge Base	Vendor Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10683

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	12.1x47	All	All	All
Operating System	Juniper	Junos	12.1x47	d10	All	All
Operating System	Juniper	Junos	12.1x47	d20	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	d5	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	12.1x47	All	All	All
Operating System	Juniper	Junos	12.1x47	d10	All	All
Operating System	Juniper	Junos	12.1x47	d20	All	All

Operating System	Juniper	Junos	12.1x47	d20	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	d5	All	All
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:12.1x47:*****:						
cpe:2.3:o:juniper:junos:12.1x47:d10:*****:						
cpe:2.3:o:juniper:junos:12.1x47:d20:*****:						
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:d5:*****:						
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:12.1x47:*****:						
cpe:2.3:o:juniper:junos:12.1x47:d10:*****:						
cpe:2.3:o:juniper:junos:12.1x47:d20:*****:						
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:d5:*****:						

No vendor comments have been submitted for this CVE

[← 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](#)