

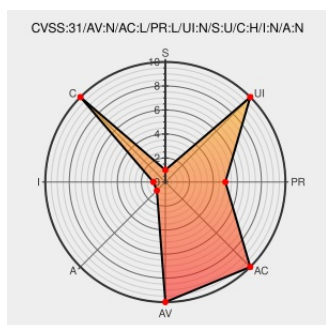


CVE-2015-3006

Published on: 02/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-3006 - advisory for JSA10678

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

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

On the QFX3500 and QFX3600 platforms, the number of bytes collected from the RANDOM_INTERRUPT entropy source when the device boots up is insufficient, possibly leading to weak or duplicate SSH keys or self-signed SSL/TLS certificates. Entropy increases after the system has been up and running for some time, but immediately

after boot, the entropy is very low. This issue only affects the QFX3500 and QFX3600 switches. No other Juniper Networks products or platforms are affected by this weak entropy vulnerability.

CVE-2015-3006 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

Vulnerability Patch/Work Around

Avoid generating SSH keys or self-signed SSL certificates on the affected platforms until the system has been up and running for some time, allowing additional sources of randomness to generate sufficient entropy.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **6.8 - MEDIUM**

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

COMPLETE

NONE

NONE

CVE References

Description

Tags

Link

2015-04 Security Bulletin: Junos: Insufficient entropy on QFX3500 and QFX3600 platforms when the system boots up (CVE-2015-3006) - Juniper Networks

Vendor Advisory

kb.juniper.net

text/html

 CONFIRM

kb.juniper.net/JSA10678

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	12.2x50	d10	All	All
Operating System	Juniper	Junos	12.2x50	d20	All	All
Operating System	Juniper	Junos	12.2x50	d41.1	All	All
Operating System	Juniper	Junos	12.2x50	d42.1	All	All
Operating System	Juniper	Junos	12.2x50	d56.1	All	All
Operating System	Juniper	Junos	13.1x50	d10	All	All
Operating System	Juniper	Junos	13.1x50	d25	All	All
Operating System	Juniper	Junos	13.2x51	d15	All	All
Operating System	Juniper	Junos	13.2x51	d20	All	All
Operating System	Juniper	Junos	13.2x51	d20.2	All	All
Operating System	Juniper	Junos	13.2x51	d21	All	All
Operating System	Juniper	Junos	13.2x52	d10	All	All
Operating System	Juniper	Junos	13.2x52	d5	All	All
Operating System	Juniper	Junos	14.1x53	-	All	All

Operating System	Juniper	Junos	12.2x50	d10	All	All
Operating System	Juniper	Junos	12.2x50	d20	All	All
Operating System	Juniper	Junos	12.2x50	d41.1	All	All
Operating System	Juniper	Junos	12.2x50	d42.1	All	All
Operating System	Juniper	Junos	12.2x50	d56.1	All	All
Operating System	Juniper	Junos	13.1x50	d10	All	All
Operating System	Juniper	Junos	13.1x50	d25	All	All
Operating System	Juniper	Junos	13.2x51	d15	All	All
Operating System	Juniper	Junos	13.2x51	d20	All	All
Operating System	Juniper	Junos	13.2x51	d20.2	All	All
Operating System	Juniper	Junos	13.2x51	d21	All	All
Operating System	Juniper	Junos	13.2x52	d10	All	All
Operating System	Juniper	Junos	13.2x52	d5	All	All
Operating System	Juniper	Junos	14.1x53	-	All	All
Hardware  	Juniper	Qfx3500	-	All	All	All
Hardware  	Juniper	Qfx3500	-	All	All	All
Hardware  	Juniper	Qfx3600	-	All	All	All
Hardware  	Juniper	Qfx3600	-	All	All	All
cpe:2.3:o:juniper:junos:12.2x50:d10:*****:						
cpe:2.3:o:juniper:junos:12.2x50:d20:*****:						
cpe:2.3:o:juniper:junos:12.2x50:d41.1:*****:						
cpe:2.3:o:juniper:junos:12.2x50:d42.1:*****:						
cpe:2.3:o:juniper:junos:12.2x50:d56.1:*****:						
cpe:2.3:o:juniper:junos:13.1x50:d10:*****:						
cpe:2.3:o:juniper:junos:13.1x50:d25:*****:						

cpe:2.3:o:juniper:junos:13.2x51:d15:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d20:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d20.2:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d21:~::~:
cpe:2.3:o:juniper:junos:13.2x52:d10:~::~:
cpe:2.3:o:juniper:junos:13.2x52:d5:~::~:
cpe:2.3:o:juniper:junos:14.1x53:-~::~:
cpe:2.3:o:juniper:junos:12.2x50:d10:~::~:
cpe:2.3:o:juniper:junos:12.2x50:d20:~::~:
cpe:2.3:o:juniper:junos:12.2x50:d41.1:~::~:
cpe:2.3:o:juniper:junos:12.2x50:d42.1:~::~:
cpe:2.3:o:juniper:junos:12.2x50:d56.1:~::~:
cpe:2.3:o:juniper:junos:13.1x50:d10:~::~:
cpe:2.3:o:juniper:junos:13.1x50:d25:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d15:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d20:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d20.2:~::~:
cpe:2.3:o:juniper:junos:13.2x51:d21:~::~:
cpe:2.3:o:juniper:junos:13.2x52:d10:~::~:
cpe:2.3:o:juniper:junos:13.2x52:d5:~::~:
cpe:2.3:o:juniper:junos:14.1x53:-~::~:
cpe:2.3:h:juniper:qfx3500:-~::~:
cpe:2.3:h:juniper:qfx3500:-~::~:
cpe:2.3:h:juniper:qfx3600:-~::~:
cpe:2.3:h:juniper:qfx3600:-~::~:

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](#)