



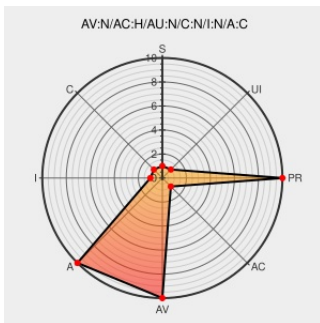
Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3822

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Juniper Junos 11.4 before 11.4R8, 12.1 before 12.1R5, 12.1X44 before 12.1X44-D20, 12.1X45 before 12.1X45-D15, 12.1X46 before 12.1X46-D10, and 12.1X47 before 12.1X47-D10 on SRX Series devices, allows remote attackers to cause a denial of service (flowd crash) via a malformed packet, related to translating IPv6 to IPv4.

CVE-2014-3822 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Juniper Networks - 2014-07 Security Bulletin: Junos: Malformed packet can cause SRX denial of service when translating traffic from IPv6 to IPv4 (CVE-2014-3822) - Knowledge Base	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10641
Juniper Junos SRX Series IPv6/IPv4 Translation flowd Bug Lets Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1030560

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

There are currently no CVEs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	11.4	All	All	All
Operating System	Juniper	Junos	12.1	All	All	All
Operating System	Juniper	Junos	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x45	All	All	All
Operating System	Juniper	Junos	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x47	All	All	All
Operating System	Juniper	Junos	11.4	All	All	All
Operating System	Juniper	Junos	12.1	All	All	All
Operating System	Juniper	Junos	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x45	All	All	All
Operating System	Juniper	Junos	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x47	All	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
Hardware	 	Juniper	Srx3600	-	All	All	All
Hardware	 	Juniper	Srx3600	-	All	All	All
Hardware	 	Juniper	Srx550	-	All	All	All
Hardware	 	Juniper	Srx550	-	All	All	All
Hardware	 	Juniper	Srx5600	-	All	All	All
Hardware	 	Juniper	Srx5600	-	All	All	All
Hardware	 	Juniper	Srx5800	-	All	All	All
Hardware	 	Juniper	Srx5800	-	All	All	All
Hardware	 	Juniper	Srx650	-	All	All	All
Hardware	 	Juniper	Srx650	-	All	All	All
cpe:2.3:o:juniper:junos:11.4:*****:							
cpe:2.3:o:juniper:junos:12.1:*****:							
cpe:2.3:o:juniper:junos:12.1x44:*****:							
cpe:2.3:o:juniper:junos:12.1x45:*****:							
cpe:2.3:o:juniper:junos:12.1x46:*****:							
cpe:2.3:o:juniper:junos:12.1x47:*****:							
cpe:2.3:o:juniper:junos:11.4:*****:							
cpe:2.3:o:juniper:junos:12.1:*****:							
cpe:2.3:o:juniper:junos:12.1x44:*****:							
cpe:2.3:o:juniper:junos:12.1x45:*****:							
cpe:2.3:o:juniper:junos:12.1x46:*****:							
cpe:2.3:o:juniper:junos:12.1x47:*****:							
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: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:-:*~::~

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