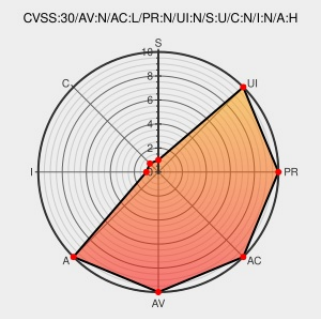
CVE-2017-10619

Published on: 10/13/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-10619

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Junos from Juniper contain the following vulnerability:

When Express Path (formerly known as service offloading) is configured on Juniper Networks SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800 in high availability cluster configuration mode, certain multicast packets might cause the flowd process to crash, halting or interrupting traffic from flowing through the device and triggering RG1+ (data-plane) fail-over to the secondary node. Repeated crashes of the flowd process may constitute an extended denial of service condition. This service is not enabled by default and is only supported in high-end SRX platforms. Affected releases are Juniper Networks Junos OS 12.3X48 prior to 12.3X48-D45, 15.1X49 prior to 15.1X49-D80 on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800.

CVE-2017-10619 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **12.3X48 prior to 12.3X48-D45**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **15.1X49 prior to 15.1X49-D80**

Vulnerability Patch/Work Around

There are no viable workarounds for this issue.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
2017-10 Security Bulletin: Junos: SRX cluster denial of service vulnerability in flowd due to multicast packets (CVE-2017-10619) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA10821

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	12.3x48	All	All	All
Operating System	Juniper	Junos	15.1x49	All	All	All
Operating System	Juniper	Junos	12.3x48	All	All	All
Operating System	Juniper	Junos	15.1x49	All	All	All
Hardware	Juniper	Srx1400	-	All	All	All
Hardware	Juniper	Srx1400	-	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	Srx5400	-	All	All	All
Hardware	Juniper	Srx5400	-	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

cpe:2.3:o:juniper:junos:12.3x48:*:*:*:*:*:*:*
cpe:2.3:o:juniper:junos:15.1x49:*:*:*:*:*:*:*
cpe:2.3:o:juniper:junos:12.3x48:*:*:*:*:*:*:*
cpe:2.3:o:juniper:junos:15.1x49:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx1400:-:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx1400:-:*:*:*:*:*:*:*
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:srx5400:-:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx5400:-:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx5600:-:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx5600:-:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx5800:-:*:*:*:*:*:*:*
cpe:2.3:h:juniper:srx5800:-:*:*:*:*:*:*:*

← Previous ID

Next ID→