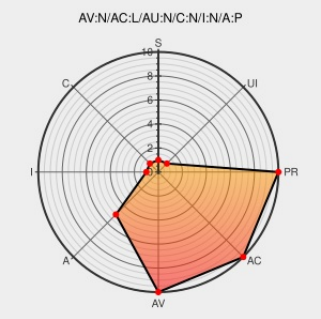
CVE-2015-7748

Published on: 10/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7748

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



Certain versions of Junos from Juniper contain the following vulnerability:

Juniper chassis with Trio (Trinity) chipset line cards and Junos OS 13.3 before 13.3R8, 14.1 before 14.1R6, 14.2 before 14.2R5, and 15.1 before 15.1R2 allow remote attackers to cause a denial of service (MPC line card crash) via a crafted uBFD packet.

CVE-2015-7748 has been assigned by cve@mitre.org to track the vulnerability

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
Juniper Junos Trio (Trinity) Chipset uBFD Packet Processing Flaw Lets Remote Users Cause the Target System to Crash - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1033858
Malformed Request	cve.report (archive), text/html	BID 101103
2015-10 Security Bulletin: Junos: Trio Chipset (Trinity) Denial of service due to maliciously crafted uBFD packet. (CVE-2015-7748) - Juniper Networks	Vendor Advisory, kb.juniper.net, text/html	CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10701

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	13.3	All	All	All
Operating System	Juniper	Junos	13.3	r1	All	All
Operating System	Juniper	Junos	13.3	r2	All	All
Operating System	Juniper	Junos	13.3	r2-s2	All	All
Operating System	Juniper	Junos	13.3	r3	All	All
Operating System	Juniper	Junos	13.3	r4	All	All
Operating System	Juniper	Junos	13.3	r5	All	All
Operating System	Juniper	Junos	13.3	r6	All	All
Operating System	Juniper	Junos	13.3	r7	All	All
Operating System	Juniper	Junos	14.1	All	All	All
Operating System	Juniper	Junos	14.1	r1	All	All
Operating System	Juniper	Junos	14.1	r2	All	All
Operating System	Juniper	Junos	14.1	r3	All	All
Operating System	Juniper	Junos	14.1	r4	All	All
Operating System	Juniper	Junos	14.1	r5	All	All
Operating System	Juniper	Junos	14.2	r1	All	All
Operating System	Juniper	Junos	14.2	r2	All	All
Operating System	Juniper	Junos	14.2	r3	All	All
Operating System	Juniper	Junos	14.2	r4	All	All
Operating System	Juniper	Junos	15.1	All	All	All

System						
Operating System	Juniper	Junos	15.1	r1	All	All
Operating System	Juniper	Junos	13.3	All	All	All
Operating System	Juniper	Junos	13.3	r1	All	All
Operating System	Juniper	Junos	13.3	r2	All	All
Operating System	Juniper	Junos	13.3	r2-s2	All	All
Operating System	Juniper	Junos	13.3	r3	All	All
Operating System	Juniper	Junos	13.3	r4	All	All
Operating System	Juniper	Junos	13.3	r5	All	All
Operating System	Juniper	Junos	13.3	r6	All	All
Operating System	Juniper	Junos	13.3	r7	All	All
Operating System	Juniper	Junos	14.1	All	All	All
Operating System	Juniper	Junos	14.1	r1	All	All
Operating System	Juniper	Junos	14.1	r2	All	All
Operating System	Juniper	Junos	14.1	r3	All	All
Operating System	Juniper	Junos	14.1	r4	All	All
Operating System	Juniper	Junos	14.1	r5	All	All
Operating System	Juniper	Junos	14.2	r1	All	All
Operating System	Juniper	Junos	14.2	r2	All	All
Operating System	Juniper	Junos	14.2	r3	All	All
Operating System	Juniper	Junos	14.2	r4	All	All
Operating System	Juniper	Junos	15.1	All	All	All
Operating System	Juniper	Junos	15.1	r1	All	All

cpe:2.3:o:juniper:junos:13.3:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r7:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.3:r7:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.1:r5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:14.2:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1:r1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→