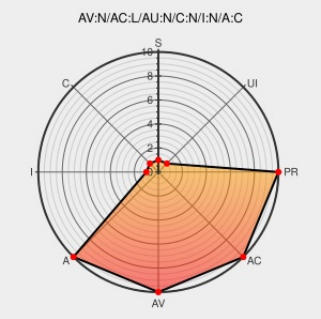
CVE-2014-3818

Published on: 10/14/2014 12:00:00 AM UTC

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

CVE-2014-3818

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



Certain versions of Junos from Juniper contain the following vulnerability:

Juniper Junos OS 9.1 through 11.4 before 11.4R11, 12.1 before R10, 12.1X44 before D40, 12.1X46 before D30, 12.1X47 before D11 and 12.147-D15, 12.1X48 before D41 and D62, 12.2 before R8, 12.2X50 before D70, 12.3 before R6, 13.1 before R4-S2, 13.1X49 before D49, 13.1X50 before 30, 13.2 before R4, 13.2X50 before D20, 13.2X51 before D25, 13.2X52 before D15, 13.3 before R2, and 14.1 before R1, when supporting 4-byte AS numbers and a BGP peer does not, allows remote attackers to cause a denial of service (memory corruption and RDP routing process crash and restart) via crafted transitive attributes in a BGP UPDATE.

CVE-2014-3818 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
2014-10 Security Bulletin: Junos: BGP UPDATE with crafted transitive attributes causes memory corruption and leads to RPD core (CVE-2014-3818) - Juniper Networks	Vendor Advisory, kb.juniper.net, text/html	CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10653
Juniper Junos BGP UPDATE Processing Flaw Lets Remote Users Deny Service - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1031009

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	10.0	All	All	All
Operating System	Juniper	Junos	10.1	All	All	All
Operating System	Juniper	Junos	10.2	All	All	All
Operating System	Juniper	Junos	10.3	All	All	All
Operating System	Juniper	Junos	10.4	All	All	All
Operating System	Juniper	Junos	10.4r	All	All	All
Operating System	Juniper	Junos	10.4s	All	All	All
Operating System	Juniper	Junos	11.0	All	All	All
Operating System	Juniper	Junos	11.1	All	All	All
Operating System	Juniper	Junos	11.2	All	All	All
Operating System	Juniper	Junos	11.3	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	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x47	All	All	All
Operating System	Juniper	Junos	12.1x48	All	All	All
Operating System	Juniper	Junos	12.2	All	All	All
Operating System	Juniper	Junos	12.2x50	All	All	All

Operating System	Juniper	Junos	12.3	All	All	All
Operating System	Juniper	Junos	13.1	All	All	All
Operating System	Juniper	Junos	13.1x49	All	All	All
Operating System	Juniper	Junos	13.1x50	All	All	All
Operating System	Juniper	Junos	13.2	All	All	All
Operating System	Juniper	Junos	13.2x50	All	All	All
Operating System	Juniper	Junos	13.2x51	All	All	All
Operating System	Juniper	Junos	13.2x52	All	All	All
Operating System	Juniper	Junos	13.3	All	All	All
Operating System	Juniper	Junos	14.1	All	All	All
Operating System	Juniper	Junos	9.1	All	All	All
Operating System	Juniper	Junos	9.2	All	All	All
Operating System	Juniper	Junos	9.4	All	All	All
Operating System	Juniper	Junos	9.5	All	All	All
Operating System	Juniper	Junos	9.6	All	All	All
Operating System	Juniper	Junos	10.0	All	All	All
Operating System	Juniper	Junos	10.1	All	All	All
Operating System	Juniper	Junos	10.2	All	All	All
Operating System	Juniper	Junos	10.3	All	All	All
Operating System	Juniper	Junos	10.4	All	All	All
Operating System	Juniper	Junos	10.4r	All	All	All
Operating System	Juniper	Junos	10.4s	All	All	All
Operating System	Juniper	Junos	11.0	All	All	All

Operating System	Juniper	Junos	11.1	All	All	All
Operating System	Juniper	Junos	11.2	All	All	All
Operating System	Juniper	Junos	11.3	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	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x47	All	All	All
Operating System	Juniper	Junos	12.1x48	All	All	All
Operating System	Juniper	Junos	12.2	All	All	All
Operating System	Juniper	Junos	12.2x50	All	All	All
Operating System	Juniper	Junos	12.3	All	All	All
Operating System	Juniper	Junos	13.1	All	All	All
Operating System	Juniper	Junos	13.1x49	All	All	All
Operating System	Juniper	Junos	13.1x50	All	All	All
Operating System	Juniper	Junos	13.2	All	All	All
Operating System	Juniper	Junos	13.2x50	All	All	All
Operating System	Juniper	Junos	13.2x51	All	All	All
Operating System	Juniper	Junos	13.2x52	All	All	All
Operating System	Juniper	Junos	13.3	All	All	All
Operating System	Juniper	Junos	14.1	All	All	All
Operating System	Juniper	Junos	9.1	All	All	All
Operating System	Juniper	Junos	9.2	All	All	All

System						
Operating System	Juniper	Junos	9.4	All	All	All
Operating System	Juniper	Junos	9.5	All	All	All
Operating System	Juniper	Junos	9.6	All	All	All

cpe:2.3:o:juniper:junos:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.3:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.4:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.4r:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.4s:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.0:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.3:*:*:*:*:*:*:*:

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:12.1x46:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.1x47:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.1x48:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.2x50:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.1x49:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.1x50:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2x50:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2x51:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2x52:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:juniper:junos:9.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.4:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.5:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.6:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.3:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.4:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.4r:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:10.4s:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.0:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:11.3:*:*:*:*:*:*:*:

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:12.1x46:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.1x47:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.1x48:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.2x50:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.1x49:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.1x50:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2x50:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2x51:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:13.2x52:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:juniper:junos:9.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.2:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.4:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.5:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:9.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→