



CVE-2013-6013

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-6013
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-17 23:55:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	Buffer overflow in the flow daemon (flowd) in Juniper Junos 10.4 before 10.4S14, 11.4 before 11.4R7-S2, 12.1.X44 before

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	11.4	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	4.0	All	All	All
Operating System	Juniper	Junos	4.1	All	All	All
Operating System	Juniper	Junos	4.2	All	All	All
Operating System	Juniper	Junos	4.3	All	All	All
Operating System	Juniper	Junos	4.4	All	All	All
Operating System	Juniper	Junos	5.0	All	All	All
Operating System	Juniper	Junos	5.1	All	All	All
Operating System	Juniper	Junos	5.2	All	All	All
Operating System	Juniper	Junos	5.3	All	All	All
Operating System	Juniper	Junos	5.4	All	All	All
Operating System	Juniper	Junos	5.5	All	All	All
Operating System	Juniper	Junos	5.6	All	All	All
Operating System	Juniper	Junos	5.7	All	All	All
Operating System	Juniper	Junos	6.0	All	All	All

Operating System	Juniper	Junos	6.1	All	All	All
Operating System	Juniper	Junos	6.2	All	All	All
Operating System	Juniper	Junos	6.3	All	All	All
Operating System	Juniper	Junos	6.4	All	All	All
Operating System	Juniper	Junos	7.0	All	All	All
Operating System	Juniper	Junos	7.1	All	All	All
Operating System	Juniper	Junos	7.2	All	All	All
Operating System	Juniper	Junos	7.3	All	All	All
Operating System	Juniper	Junos	7.4	All	All	All
Operating System	Juniper	Junos	7.5	All	All	All
Operating System	Juniper	Junos	7.6	All	All	All
Operating System	Juniper	Junos	8.0	All	All	All
Operating System	Juniper	Junos	8.1	All	All	All
Operating System	Juniper	Junos	8.2	All	All	All
Operating System	Juniper	Junos	8.3	All	All	All
Operating System	Juniper	Junos	8.4	All	All	All
Operating System	Juniper	Junos	9.0	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	11.4	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	4.0	All	All	All
Operating System	Juniper	Junos	4.1	All	All	All
Operating System	Juniper	Junos	4.2	All	All	All
Operating System	Juniper	Junos	4.3	All	All	All
Operating System	Juniper	Junos	4.4	All	All	All
Operating System	Juniper	Junos	5.0	All	All	All
Operating System	Juniper	Junos	5.1	All	All	All
Operating System	Juniper	Junos	5.2	All	All	All
Operating System	Juniper	Junos	5.3	All	All	All
Operating System	Juniper	Junos	5.4	All	All	All

Operating System	Juniper	Junos	5.5	All	All	All
Operating System	Juniper	Junos	5.6	All	All	All
Operating System	Juniper	Junos	5.7	All	All	All
Operating System	Juniper	Junos	6.0	All	All	All
Operating System	Juniper	Junos	6.1	All	All	All
Operating System	Juniper	Junos	6.2	All	All	All
Operating System	Juniper	Junos	6.3	All	All	All
Operating System	Juniper	Junos	6.4	All	All	All
Operating System	Juniper	Junos	7.0	All	All	All
Operating System	Juniper	Junos	7.1	All	All	All
Operating System	Juniper	Junos	7.2	All	All	All
Operating System	Juniper	Junos	7.3	All	All	All
Operating System	Juniper	Junos	7.4	All	All	All
Operating System	Juniper	Junos	7.5	All	All	All
Operating System	Juniper	Junos	7.6	All	All	All
Operating System	Juniper	Junos	8.0	All	All	All
Operating System	Juniper	Junos	8.1	All	All	All
Operating System	Juniper	Junos	8.2	All	All	All
Operating System	Juniper	Junos	8.3	All	All	All
Operating System	Juniper	Junos	8.4	All	All	All
Operating System	Juniper	Junos	9.0	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	All	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
Operating System	Juniper	Junos	All	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

References

Reference
Juniper Networks Junos Telnet Messages Remote Buffer Overflow Vulnerability
About Secunia Research Flexera
98369
Juniper Networks - 2013-10 Security Bulletin: Junos: SRX flowd core due to buffer overflow while processing telnet protocol (CVE-2013-6013)
Juniper Junos SRX Series Gateway Buffer Overflow in Telnet Firewall Lets Remote Users Execute Arbitrary Code - SecurityTracker
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report