CVE-2013-6618

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-6618
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-05 20:55:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	jsdm/ajax/port.php in J-Web in Juniper Junos before 10.4R13, 11.4 before 11.4R7, 12.1 before 12.1R5, 12.2 before 12.2R3

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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	11.4	All	All	All
Operating System	Juniper	Junos	12.1	All	All	All
Operating System	Juniper	Junos	12.2	All	All	All
Operating System	Juniper	Junos	12.3	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	11.4	All	All	All
Operating System	Juniper	Junos	12.1	All	All	All
Operating System	Juniper	Junos	12.2	All	All	All
Operating System	Juniper	Junos	12.3	All	All	All
Operating System	Juniper	Junos	All	All	All	All

References

Reference	Source
Juniper Junos J-Web Privilege Escalation Vulnerability	BID
Juniper Junos J-Web '/jsdm/ajax/port.php' Script Lets Remote Authenticated Users Execute Arbitrary Commands - SecurityTracker	SECTR
About Secunia Research | Flexera	SECUN
Juniper Networks - 2013-04 Security Bulletin: Junos: J-Web Sajax remote code execution - Knowledge Base	CONFIF
Juniper Junos J-Web - Privilege Escalation Vulnerability	EXPLO
Sense of Security - Security Advisory - SOS-13-003 - Juniper Junos J-Web Privilege Escalation Vulnerability	MISC
IBM X-Force Exchange	XF
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
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 registred 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**