



CVE-2013-6012

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

Summary

CVE	CVE-2013-6012
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-28 22:55:00 UTC
Updated	2013-11-03 03:34:00 UTC
Description	Juniper Junos 12.1X44 before 12.1.X44-D20 and 12.1X45 before 12.1X45-D15, when the no-validate option is enabled, do

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x45	All	All	All
Operating System	Juniper	Junos	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x45	All	All	All

References

Reference
Juniper Networks - 2013-10 Security Bulletin: Junos: Commit failure on SRX after upgrade to 12.1X44 or 12.1X45 may allow unauthenticated
Juniper Junos Config Commit Phase CVE-2013-6012 Remote Authentication Bypass Vulnerability
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.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 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](#)