



CVE-2015-0236

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

Summary

CVE	CVE-2015-0236
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-29 15:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	libvirt before 1.2.12 allow remote authenticated users to obtain the VNC password by using the VIR_DOMAIN_XML_SECU

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Mageia	Mageia	4.0	All	All	All
Operating System	Mageia	Mageia	4.0	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Libvirt	1.2.0	All	All	All
Application	Redhat	Libvirt	1.2.1	All	All	All
Application	Redhat	Libvirt	1.2.10	All	All	All
Application	Redhat	Libvirt	1.2.2	All	All	All
Application	Redhat	Libvirt	1.2.3	All	All	All
Application	Redhat	Libvirt	1.2.4	All	All	All
Application	Redhat	Libvirt	1.2.5	All	All	All
Application	Redhat	Libvirt	1.2.6	All	All	All
Application	Redhat	Libvirt	1.2.7	All	All	All
Application	Redhat	Libvirt	1.2.8	All	All	All
Application	Redhat	Libvirt	1.2.9	All	All	All
Application	Redhat	Libvirt	1.2.0	All	All	All
Application	Redhat	Libvirt	1.2.1	All	All	All
Application	Redhat	Libvirt	1.2.10	All	All	All
Application	Redhat	Libvirt	1.2.2	All	All	All
Application	Redhat	Libvirt	1.2.3	All	All	All
Application	Redhat	Libvirt	1.2.4	All	All	All
Application	Redhat	Libvirt	1.2.5	All	All	All
Application	Redhat	Libvirt	1.2.6	All	All	All
Application	Redhat	Libvirt	1.2.7	All	All	All
Application	Redhat	Libvirt	1.2.8	All	All	All
Application	Redhat	Libvirt	1.2.9	All	All	All
Application	Redhat	Libvirt	All	All	All	All

References

Reference

Libvirt Security Notice: LSN-2015-0001

Red Hat Customer Portal

openSUSE-SU-2015:0225-1: moderate: Security update for libvirt

Security Advisory SA62766 - SUSE update for libvirt - Secunia

[access.redhat.com](#) | [CVE-2015-0236](#)

1184431 – (CVE-2015-0236) CVE-2015-0236 libvirt: missing ACL check for the VIR_DOMAIN_XML_SECURE flag in save images and snaps

[USN-2867-1: libvirt vulnerabilities](#) | [Ubuntu](#)

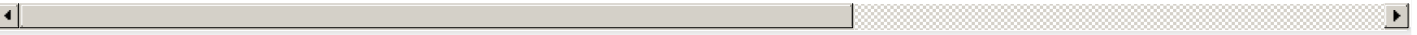
[Support / Security / Advisories // MDVSA-2015:070](#) | [Mandriva](#)

[Support / Security / Advisories // MDVSA-2015:035](#) | [Mandriva](#)

[Mageia Advisory: MGASA-2015-0046 - Updated libvirt packages fix CVE-2015-0236](#)

[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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)