

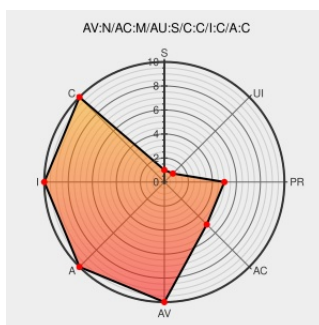


CVE-2013-4401

Published on: 11/02/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:46:00 AM UTC

CVE-2013-4401

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Libvirt](#) from [Redhat](#) contain the following vulnerability:

The `virConnectDomainXMLToNative` API function in `libvirt 1.1.0` through `1.1.3` checks for the `connect:read` permission instead of the `connect:write` permission, which allows attackers to gain `domain:write` privileges and execute `Qemu` binaries via crafted XML. NOTE: some of these details are obtained from third party information.

CVE-2013-4401 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **8.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

SINGLE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

libvirt.org Git -
libvirt.git/commit

[web.archive.org](#)

[text/xml](#)

[Inactive Link](#)

[Not Archived](#)

[MISC libvirt.org/git/?p=libvirt.git%3Ba=commit%3Bh=57687fd6bf7f6e1b3662c52f3f26c06ab19dc96c](#)

1015259 – (CVE-2013-4401)
CVE-2013-4401 libvirt:
unintended API access due to
incorrect permissions checks

[Patch](#)

[bugzilla.redhat.com](#)

[text/html](#)

[MISC bugzilla.redhat.com/show_bug.cgi?id=1015259](#)

Gentoo Linux Documentation
-- libvirt: Multiple
vulnerabilities

[security.gentoo.org](#)

[text/html](#)

[GENTOO GLSA-201412-04](#)

libvirt: Wiki: Maintenance
Releases

[wiki.libvirt.org](#)

[text/html](#)

[CONFIRM wiki.libvirt.org/page/Maintenance_Releases](#)

USN-2026-1: libvirt vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2026-1
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	web.archive.org text/html	 SECUNIA 60895
libvirt API Access Control Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1029241
Security Advisory SA55210 - libvirt Privilege Escalation and Security Bypass Vulnerabilities - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 55210

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
Application	Redhat	Libvirt	1.1.0	All	All	All
Application	Redhat	Libvirt	1.1.1	All	All	All
Application	Redhat	Libvirt	1.1.2	All	All	All
Application	Redhat	Libvirt	1.1.3	All	All	All
Application	Redhat	Libvirt	1.1.0	All	All	All
Application	Redhat	Libvirt	1.1.1	All	All	All
Application	Redhat	Libvirt	1.1.2	All	All	All
Application	Redhat	Libvirt	1.1.3	All	All	All
cpe:2.3:a:redhat:libvirt:1.1.0:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.1:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.2:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.3:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.0:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.1:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.2:*****.*.*.*						
cpe:2.3:a:redhat:libvirt:1.1.3:*****.*.*.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

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](#)