



CVE-2014-3672

Published on: 05/25/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:41:00 AM UTC

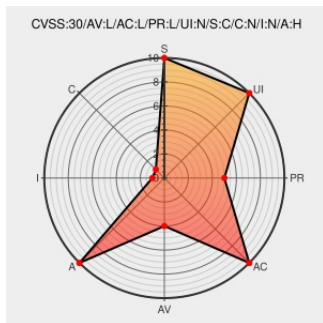
CVE-2014-3672

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The qemu implementation in libvirt before 1.3.0 and Xen allows local guest OS users to cause a denial of service (host disk consumption) by writing to stdout or stderr.

CVE-2014-3672 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
XSA-180 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-180.html
libvirt: Releases (2015)	Release Notes	CONFIRM libvirt.org/news-2015.html

Vendor Advisory
web.archive.org
text/xml
Inactive Link Not Archived

Xen libxl Logging Lets
Local Users on a Guest
System Cause Denial of
Service Conditions on the
Guest System -
SecurityTracker

Third Party Advisory
VDB Entry
www.securitytracker.com
text/html

SECTRAK 1035945

Oracle VM Server for x86
Bulletin - July 2016

Third Party Advisory
web.archive.org
text/html
Inactive Link Not Archived

CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html

libvirt.org Git -
libvirt.git/commit

Vendor Advisory
web.archive.org
text/xml
Inactive Link Not Archived

MISC libvirt.org/git/?
p=libvirt.git%3Ba=commit%3Bh=0d968ad715475a1660779bcdd2c5b38ad63db4cf

oss-security - CVE-2014-
3672 libvirt: DoS via
excessive logging

Mailing List
www.openwall.com
text/html

MLIST [oss-security] 20160524 CVE-2014-3672 libvirt: DoS via excessive logging

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	All	All	All	All
Operating System	Xen	Xen	All	All	All	All
Operating System	Xen	Xen	All	All	All	All
cpe:2.3:a:redhat:libvirt:*****:						
cpe:2.3:o:xen:xen:*****:						
cpe:2.3:o:xen:xen:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)