

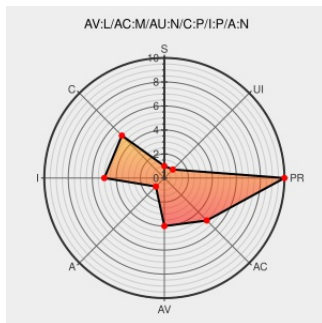


CVE-2013-1922

Published on: 05/13/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:14 AM UTC

CVE-2013-1922

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

Certain versions of [Xen](#) from [Xen](#) contain the following vulnerability: qemu-nbd in QEMU, as used in Xen 4.2.x, determines the format of a raw disk image based on the header, which allows local guest OS administrators to read arbitrary files on the host by modifying the header to identify a different format, which is used when the guest is restarted, a different vulnerability than CVE-2008-2004.

CVE-2013-1922 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.3 - LOW**

Access Vector

LOCAL

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

[SECURITY] Fedora 18 Update: qemu-1.2.2-11.fc18

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

[FEDORA FEDORA-2013-6221](#)

oss-security - CVE-2013-1922 -- qemu: qemu-nbd block format auto-detection vulnerability

[www.openwall.com](https://www.openwall.com/text/html)
text/html

[MLIST \[oss-security\] 20130416 CVE-2013-1922 -- qemu: qemu-nbd block format auto-detection vulnerability](#)

Xen qemu-nbd-xen Format Detection Flaw Lets Local Guest Users Access Files on the Host - SecurityTracker

[www.securitytracker.com](https://www.securitytracker.com/text/html)
text/html

[SECTrack 1028426](#)

[SECURITY] Fedora 17 Update: qemu-1.0.1-6.fc17

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

[FEDORA FEDORA-2013-6211](#)

Security Advisory SA55082 - Gentoo update for xen - Secunia

[web.archive.org](https://web.archive.org/text/html)
text/html

[SECUNIA 55082](#)

Gentoo Linux Documentation -- Xen: Multiple

security.gentoo.org

[GENTOO GLSA-201309-24](#)

vulnerabilities

oss-security - Xen Security Advisory 48 (CVE-2013-1922)
- qemu-nbd format-guessing due to missing format specification

[SECURITY] Fedora 19 Update: qemu-1.4.1-1.fc19

text/html

www.openwall.com

text/html

MLIST [oss-security] 20130415 Xen Security Advisory 48 (CVE-2013-1922) - qemu-nbd format-guessing due to missing format specification

lists.fedoraproject.org

text/html

FEDORA FEDORA-2013-6185

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
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
cpe:2.3:o:xen:xen:4.2.0:*****:						
cpe:2.3:o:xen:xen:4.2.1:*****:						
cpe:2.3:o:xen:xen:4.2.2:*****:						
cpe:2.3:o:xen:xen:4.2.0:*****:						
cpe:2.3:o:xen:xen:4.2.1:*****:						
cpe:2.3:o:xen:xen:4.2.2:*****:						

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](#)