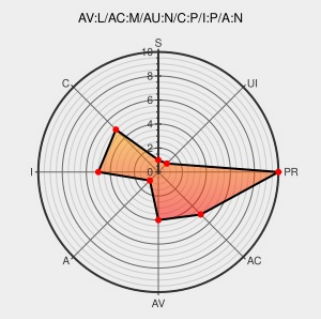
CVE-2013-1922

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	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
[SECURITY] Fedora 18 Update: qemu-1.2.2-11.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6221
oss-security - CVE-2013-1922 -- qemu: qemu-nbd block format auto-detection vulnerability	www.openwall.com 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 text/html	SECTRACK 1028426
[SECURITY] Fedora 17 Update: qemu-1.0.1-6.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6211
Security Advisory SA55082 - Gentoo update for xen - Secunia	web.archive.org text/html	SECUNIA 55082
Gentoo Linux Documentation -- Xen: Multiple	security.gentoo.org	GENTOO GLSA-201309-24

vulnerabilities	text/html	
oss-security - Xen Security Advisory 48 (CVE-2013-1922) - qemu-nbd format-guessing due to missing format specification	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
[SECURITY] Fedora 19 Update: qemu-1.4.1-1.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6185

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 and Source URL Uptime Status status.cve.report