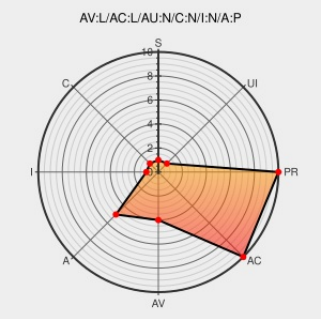
CVE-2013-6436

Published on: 01/07/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:29:00 AM UTC

CVE-2013-6436

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libvirt from Redhat contain the following vulnerability:

The lxcDomainGetMemoryParameters method in lxc/lxc_driver.c in libvirt 1.0.5 through 1.2.0 does not properly check the status of LXC guests when reading memory tunables, which allows local users to cause a denial of service (NULL pointer dereference and libvirtd crash) via a guest in the shutdown status, as demonstrated by the "virsh memtune" command.

CVE-2013-6436 has been assigned by secalert@redhat.com to track the vulnerability

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
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=f8c1cb90213508c4f32549023b0572ed77
[libvirt] SECURITY: CVE-2013-6436: libvirtd daemon crash when reading me	www.redhat.com, text/html	MLIST [libvirt] 20131220 SECURITY: CVE-2013-6436: libvirtd daemon when reading memory tunables for LXC guest in shutoff status
USN-2093-1: libvirt vulnerabilities | Ubuntu	www.ubuntu.com, text/html	UBUNTU USN-2093-1
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities	security.gentoo.org, text/html	GENTOO GLSA-201412-04

Security Advisory SA56245 - libvirt "lxcDomainGetMemoryParameters()" Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 56245
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 101485
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	web.archive.org text/html	SECUNIA 60895
openSUSE-SU-2014:0010-1: moderate: update for libvirt	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0010

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	1.0.5	All	All	All
Application	Redhat	Libvirt	1.0.5.1	All	All	All
Application	Redhat	Libvirt	1.0.5.2	All	All	All
Application	Redhat	Libvirt	1.0.5.3	All	All	All
Application	Redhat	Libvirt	1.0.5.4	All	All	All
Application	Redhat	Libvirt	1.0.5.5	All	All	All
Application	Redhat	Libvirt	1.0.5.6	All	All	All
Application	Redhat	Libvirt	1.0.6	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
Application	Redhat	Libvirt	1.1.4	All	All	All
Application	Redhat	Libvirt	1.2.0	All	All	All
Application	Redhat	Libvirt	1.0.5	All	All	All
Application	Redhat	Libvirt	1.0.5.1	All	All	All
Application	Redhat	Libvirt	1.0.5.2	All	All	All
Application	Redhat	Libvirt	1.0.5.3	All	All	All
Application	Redhat	Libvirt	1.0.5.4	All	All	All

Application	Redhat	Libvirt	1.0.5.5	All	All	All
Application	Redhat	Libvirt	1.0.5.6	All	All	All
Application	Redhat	Libvirt	1.0.6	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
Application	Redhat	Libvirt	1.1.4	All	All	All
Application	Redhat	Libvirt	1.2.0	All	All	All

cpe:2.3:a:redhat:libvirt:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.6:*:*:*:*:*:*:*:

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:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.6:*:*:*:*:*:*:*

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:1.1.4:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→