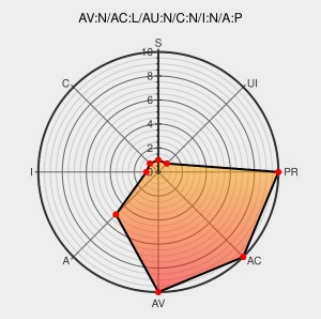
CVE-2013-4153

Published on: 09/30/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:44:00 AM UTC

CVE-2013-4153

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



Certain versions of Libvirt from Redhat contain the following vulnerability:

Double free vulnerability in the qemuAgentGetVCPUs function in qemu/qemu_agent.c in libvirt 1.0.6 through 1.1.0 allows remote attackers to cause a denial of service (daemon crash) via a cpu count request, as demonstrated by the "virsh vcpucount dom --guest" command.

CVE-2013-4153 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
libvirt.org Git - libvirt.git/commitdiff	web.archive.org text/xml Inactive Link Not Archived	MISC libvirt.org/git/?p=libvirt.git%3Ba=commitdiff%3Bh=dfc692350a04a70b4ca65667c30869b3bfdaf034
oss-security - Re: CVE request -- libvirt: double free of returned JSON array in qemuAgentGetVCPUs()	Patch openwall.com text/html	MLIST [oss-security] 20130719 Re: CVE request -- libvirt: double free of returned JSON array in qemuAgentGetVCPUs()
984821 – Crash of libvirtd without guest agent configuration	Exploit bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=984821
libvirt: Releases	libvirt.org	CONFIRM libvirt.org/news.html

	text/xml	
986383 – (CVE-2013-4153) CVE-2013-4153 libvirt: double free of returned JSON array in qemuAgentGetVCPUs()	Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=986383

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	1.0.6	All	All	All
Application	Redhat	Libvirt	1.1.0	All	All	All
Application	Redhat	Libvirt	1.0.6	All	All	All
Application	Redhat	Libvirt	1.1.0	All	All	All

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

cpe:2.3:a:redhat:libvirt:1.1.0:*:*:*:*:*:*:*:

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

cpe:2.3:a:redhat:libvirt:1.1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→