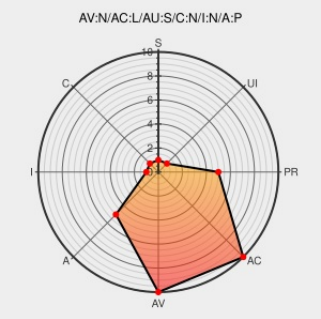
CVE-2013-4296

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

Last Modified on: 02/13/2023 12:28:00 AM UTC

CVE-2013-4296

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The remoteDispatchDomainMemoryStats function in daemon/remote.c in libvirt 0.9.1 through 0.10.1.x, 0.10.2.x before 0.10.2.8, 1.0.x before 1.0.5.6, and 1.1.x before 1.1.2 allows remote authenticated users to cause a denial of service (uninitialized pointer dereference and crash) via a crafted RPC call.

CVE-2013-4296 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:1272
1006173 – (CVE-2013-4296) CVE-2013-4296 libvirt: invalid free in remoteDispatchDomainMemoryStats	Patch, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1006173
libvirt.org Git - libvirt.git/commit	web.archive.org, text/xml, Inactive Link, Not Archived	MISC libvirt.org/git/?p=libvirt.git%3Ba=commit%3Bh=e7f400a110e2e3673b96518170bfea085
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities	security.gentoo.org, text/html	GENTOO GLSA-201412-04

libvirt: Wiki: Maintenance Releases	Patch wiki.libvirt.org text/html	CONFIRM wiki.libvirt.org/page/Maintenance_Releases
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	web.archive.org text/html	SECUNIA 60895
openSUSE-SU-2013:1550-1: moderate: libvirt: security and bugfix update	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1550
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1460
openSUSE-SU-2013:1549-1: moderate: libvirt: fixed security bugs	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1549
USN-1954-1: libvirt vulnerabilities | Ubuntu	Vendor Advisory www.ubuntu.com text/html	UBUNTU USN-1954-1
Debian -- Security Information -- DSA-2764-1 libvirt	www.debian.org Depreciated Link text/html	DEBIAN DSA-2764

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Application	Redhat	Libvirt	0.10.0	All	All	All
Application	Redhat	Libvirt	0.10.1	All	All	All
Application	Redhat	Libvirt	0.10.2	All	All	All
Application	Redhat	Libvirt	0.10.2.1	All	All	All
Application	Redhat	Libvirt	0.10.2.2	All	All	All
Application	Redhat	Libvirt	0.10.2.3	All	All	All
Application	Redhat	Libvirt	0.10.2.4	All	All	All
Application	Redhat	Libvirt	0.10.2.5	All	All	All
Application	Redhat	Libvirt	0.10.2.6	All	All	All
Application	Redhat	Libvirt	0.10.2.7	All	All	All
Application	Redhat	Libvirt	0.9.1	All	All	All
Application	Redhat	Libvirt	0.9.10	All	All	All
Application	Redhat	Libvirt	0.9.11	All	All	All
Application	Redhat	Libvirt	0.9.12	All	All	All
Application	Redhat	Libvirt	0.9.13	All	All	All
Application	Redhat	Libvirt	0.9.2	All	All	All
Application	Redhat	Libvirt	0.9.3	All	All	All
Application	Redhat	Libvirt	0.9.4	All	All	All
Application	Redhat	Libvirt	0.9.5	All	All	All
Application	Redhat	Libvirt	0.9.6	All	All	All
Application	Redhat	Libvirt	0.9.7	All	All	All
Application	Redhat	Libvirt	0.9.8	All	All	All
Application	Redhat	Libvirt	0.9.9	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	1.1.0	All	All	All
Application	Redhat	Libvirt	1.1.1	All	All	All
Application	Redhat	Libvirt	0.10.0	All	All	All
Application	Redhat	Libvirt	0.10.1	All	All	All
Application	Redhat	Libvirt	0.10.2	All	All	All

Application	Redhat	Libvirt	0.10.2.1	All	All	All
Application	Redhat	Libvirt	0.10.2.2	All	All	All
Application	Redhat	Libvirt	0.10.2.3	All	All	All
Application	Redhat	Libvirt	0.10.2.4	All	All	All
Application	Redhat	Libvirt	0.10.2.5	All	All	All
Application	Redhat	Libvirt	0.10.2.6	All	All	All
Application	Redhat	Libvirt	0.10.2.7	All	All	All
Application	Redhat	Libvirt	0.9.1	All	All	All
Application	Redhat	Libvirt	0.9.10	All	All	All
Application	Redhat	Libvirt	0.9.11	All	All	All
Application	Redhat	Libvirt	0.9.12	All	All	All
Application	Redhat	Libvirt	0.9.13	All	All	All
Application	Redhat	Libvirt	0.9.2	All	All	All
Application	Redhat	Libvirt	0.9.3	All	All	All
Application	Redhat	Libvirt	0.9.4	All	All	All
Application	Redhat	Libvirt	0.9.5	All	All	All
Application	Redhat	Libvirt	0.9.6	All	All	All
Application	Redhat	Libvirt	0.9.7	All	All	All
Application	Redhat	Libvirt	0.9.8	All	All	All
Application	Redhat	Libvirt	0.9.9	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	1.1.0	All	All	All
Application	Redhat	Libvirt	1.1.1	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.10:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.12:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.13:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.9:*:*:*:*:*:*:*:

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:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.10.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.10:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.12:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.13:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:0.9.9:*:*:*:*:*:*:*:

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:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→