

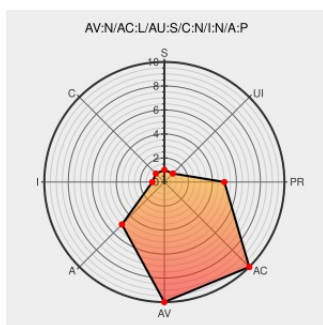


CVE-2011-2511

Published on: 08/10/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:31:00 AM UTC

CVE-2011-2511

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

Certain versions of [Libvirt](#) from [Redhat](#) contain the following vulnerability:

Integer overflow in libvirt before 0.9.3 allows remote authenticated users to cause a denial of service (libvirtd crash) and possibly execute arbitrary code via a crafted VirDomainGetVcpus RPC call that triggers memory corruption.

CVE-2011-2511 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

[access.redhat.com](https://access.redhat.com/text/html)
text/html

[MISC access.redhat.com/errata/RHSA-2011:1197](https://access.redhat.com/errata/RHSA-2011:1197)

Hermes - openSUSE Notification Client

[web.archive.org](https://web.archive.org/text/html)
text/html
Inactive Link **Not Archived**

[SUSE SUSE-SU-2011:0837](https://www.suse.com/support/update/notifications/#SUSE-SU-2011:0837)

Security Advisory SA45446 - Ubuntu update for libvirt - Secunia

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

[SECUNIA 45446](https://www.secunia.com/advisories/45446)

[SECURITY] Fedora 14 Update: libvirt-0.8.3-10.fc14

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

[FEDORA FEDORA-2011-9062](https://www.fedoraproject.org/wiki/SecurityAdvisories/FEDORA-2011-9062)

Fedora update for libvirt - Secunia.com

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

[SECUNIA 45375](https://www.secunia.com/advisories/45375)

CVE-2011-2511 - Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2011-2511
Bug 717199 – CVE-2011-2511 libvirt: integer overflow in VirDomainGetVcpus	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=717199
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2011:1019
oss-security - CVE request: libvirt: integer overflow in VirDomainGetVcpus	Patch www.openwall.com text/html	 MLIST [oss-security] 20110628 CVE request: libvirt: integer overflow in VirDomainGetVcpus
Support	Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2011:1019
Debian -- Security Information -- DSA-2280-1 libvirt	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2280
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF libvirt-virdomaingetvcpus-bo(68271)
[SECURITY] Fedora 15 Update: libvirt-0.8.8-7.fc15	lists.fedoraproject.org text/html	 FEDORA FEDORA-2011-9091
libvirt: Releases	libvirt.org text/xml	 CONFIRM libvirt.org/news.html
Support	www.redhat.com text/html	 REDHAT RHSA-2011:1197
USN-1180-1: libvirt vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1180-1
libvirt RPC Processing Integer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1025822
[libvirt] [PATCH 2/2] remote: protect against integer overflow	Patch www.redhat.com text/x-diff	 MLIST [libvirt] 20110624 [PATCH 2/2] remote: protect against integer overflow
Security Advisory SA45441 - SUSE update for libvirt - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 45441

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	0.0.1	All	All	All
Application	Redhat	Libvirt	0.0.2	All	All	All

Application	Hedhat	Libvirt	0.0.3	All	All	All
Application	Redhat	Libvirt	0.0.4	All	All	All
Application	Redhat	Libvirt	0.0.5	All	All	All
Application	Redhat	Libvirt	0.0.6	All	All	All
Application	Redhat	Libvirt	0.1.0	All	All	All
Application	Redhat	Libvirt	0.1.1	All	All	All
Application	Redhat	Libvirt	0.1.3	All	All	All
Application	Redhat	Libvirt	0.1.4	All	All	All
Application	Redhat	Libvirt	0.1.5	All	All	All
Application	Redhat	Libvirt	0.1.6	All	All	All
Application	Redhat	Libvirt	0.1.7	All	All	All
Application	Redhat	Libvirt	0.1.8	All	All	All
Application	Redhat	Libvirt	0.1.9	All	All	All
Application	Redhat	Libvirt	0.2.0	All	All	All
Application	Redhat	Libvirt	0.2.1	All	All	All
Application	Redhat	Libvirt	0.2.2	All	All	All
Application	Redhat	Libvirt	0.2.3	All	All	All
Application	Redhat	Libvirt	0.3.0	All	All	All
Application	Redhat	Libvirt	0.3.1	All	All	All
Application	Redhat	Libvirt	0.3.2	All	All	All
Application	Redhat	Libvirt	0.3.3	All	All	All
Application	Redhat	Libvirt	0.4.0	All	All	All
Application	Redhat	Libvirt	0.4.1	All	All	All
Application	Redhat	Libvirt	0.4.2	All	All	All
Application	Redhat	Libvirt	0.4.3	All	All	All
Application	Redhat	Libvirt	0.4.4	All	All	All
Application	Redhat	Libvirt	0.4.5	All	All	All
Application	Redhat	Libvirt	0.4.6	All	All	All
Application	Redhat	Libvirt	0.5.0	All	All	All
Application	Redhat	Libvirt	0.5.1	All	All	All
Application	Redhat	Libvirt	0.6.0	All	All	All
Application	Redhat	Libvirt	0.6.1	All	All	All
Application	Redhat	Libvirt	0.6.2	All	All	All
Application	Redhat	Libvirt	0.6.3	All	All	All
Application	Redhat	Libvirt	0.6.4	All	All	All
Application	Redhat	Libvirt	0.6.5	All	All	All

Application	Redhat	Libvirt	0.7.0	All	All	All
Application	Redhat	Libvirt	0.7.1	All	All	All
Application	Redhat	Libvirt	0.7.2	All	All	All
Application	Redhat	Libvirt	0.7.3	All	All	All
Application	Redhat	Libvirt	0.7.4	All	All	All
Application	Redhat	Libvirt	0.7.5	All	All	All
Application	Redhat	Libvirt	0.7.6	All	All	All
Application	Redhat	Libvirt	0.7.7	All	All	All
Application	Redhat	Libvirt	0.8.0	All	All	All
Application	Redhat	Libvirt	0.8.1	All	All	All
Application	Redhat	Libvirt	0.8.2	All	All	All
Application	Redhat	Libvirt	0.8.3	All	All	All
Application	Redhat	Libvirt	0.8.4	All	All	All
Application	Redhat	Libvirt	0.8.5	All	All	All
Application	Redhat	Libvirt	0.8.6	All	All	All
Application	Redhat	Libvirt	0.8.7	All	All	All
Application	Redhat	Libvirt	0.8.8	All	All	All
Application	Redhat	Libvirt	0.9.0	All	All	All
Application	Redhat	Libvirt	0.9.1	All	All	All
Application	Redhat	Libvirt	All	All	All	All
Application	Redhat	Libvirt	0.0.1	All	All	All
Application	Redhat	Libvirt	0.0.2	All	All	All
Application	Redhat	Libvirt	0.0.3	All	All	All
Application	Redhat	Libvirt	0.0.4	All	All	All
Application	Redhat	Libvirt	0.0.5	All	All	All
Application	Redhat	Libvirt	0.0.6	All	All	All
Application	Redhat	Libvirt	0.1.0	All	All	All
Application	Redhat	Libvirt	0.1.1	All	All	All
Application	Redhat	Libvirt	0.1.3	All	All	All
Application	Redhat	Libvirt	0.1.4	All	All	All
Application	Redhat	Libvirt	0.1.5	All	All	All
Application	Redhat	Libvirt	0.1.6	All	All	All
Application	Redhat	Libvirt	0.1.7	All	All	All
Application	Redhat	Libvirt	0.1.8	All	All	All
Application	Redhat	Libvirt	0.1.9	All	All	All

Application	Redhat	Libvirt	0.2.0	All	All	All
Application	Redhat	Libvirt	0.2.1	All	All	All
Application	Redhat	Libvirt	0.2.2	All	All	All
Application	Redhat	Libvirt	0.2.3	All	All	All
Application	Redhat	Libvirt	0.3.0	All	All	All
Application	Redhat	Libvirt	0.3.1	All	All	All
Application	Redhat	Libvirt	0.3.2	All	All	All
Application	Redhat	Libvirt	0.3.3	All	All	All
Application	Redhat	Libvirt	0.4.0	All	All	All
Application	Redhat	Libvirt	0.4.1	All	All	All
Application	Redhat	Libvirt	0.4.2	All	All	All
Application	Redhat	Libvirt	0.4.3	All	All	All
Application	Redhat	Libvirt	0.4.4	All	All	All
Application	Redhat	Libvirt	0.4.5	All	All	All
Application	Redhat	Libvirt	0.4.6	All	All	All
Application	Redhat	Libvirt	0.5.0	All	All	All
Application	Redhat	Libvirt	0.5.1	All	All	All
Application	Redhat	Libvirt	0.6.0	All	All	All
Application	Redhat	Libvirt	0.6.1	All	All	All
Application	Redhat	Libvirt	0.6.2	All	All	All
Application	Redhat	Libvirt	0.6.3	All	All	All
Application	Redhat	Libvirt	0.6.4	All	All	All
Application	Redhat	Libvirt	0.6.5	All	All	All
Application	Redhat	Libvirt	0.7.0	All	All	All
Application	Redhat	Libvirt	0.7.1	All	All	All
Application	Redhat	Libvirt	0.7.2	All	All	All
Application	Redhat	Libvirt	0.7.3	All	All	All
Application	Redhat	Libvirt	0.7.4	All	All	All
Application	Redhat	Libvirt	0.7.5	All	All	All
Application	Redhat	Libvirt	0.7.6	All	All	All
Application	Redhat	Libvirt	0.7.7	All	All	All
Application	Redhat	Libvirt	0.8.0	All	All	All
Application	Redhat	Libvirt	0.8.1	All	All	All
Application	Redhat	Libvirt	0.8.2	All	All	All
Application	Redhat	Libvirt	0.8.3	All	All	All
Application	Redhat	Libvirt	0.8.4	All	All	All

Application	Redhat	Libvirt	0.8.4	All	All	All
Application	Redhat	Libvirt	0.8.5	All	All	All
Application	Redhat	Libvirt	0.8.6	All	All	All
Application	Redhat	Libvirt	0.8.7	All	All	All
Application	Redhat	Libvirt	0.8.8	All	All	All
Application	Redhat	Libvirt	0.9.0	All	All	All
Application	Redhat	Libvirt	0.9.1	All	All	All
cpe:2.3:a:redhat:libvirt:0.0.1:*****:						
cpe:2.3:a:redhat:libvirt:0.0.2:*****:						
cpe:2.3:a:redhat:libvirt:0.0.3:*****:						
cpe:2.3:a:redhat:libvirt:0.0.4:*****:						
cpe:2.3:a:redhat:libvirt:0.0.5:*****:						
cpe:2.3:a:redhat:libvirt:0.0.6:*****:						
cpe:2.3:a:redhat:libvirt:0.1.0:*****:						
cpe:2.3:a:redhat:libvirt:0.1.1:*****:						
cpe:2.3:a:redhat:libvirt:0.1.3:*****:						
cpe:2.3:a:redhat:libvirt:0.1.4:*****:						
cpe:2.3:a:redhat:libvirt:0.1.5:*****:						
cpe:2.3:a:redhat:libvirt:0.1.6:*****:						
cpe:2.3:a:redhat:libvirt:0.1.7:*****:						
cpe:2.3:a:redhat:libvirt:0.1.8:*****:						
cpe:2.3:a:redhat:libvirt:0.1.9:*****:						
cpe:2.3:a:redhat:libvirt:0.2.0:*****:						
cpe:2.3:a:redhat:libvirt:0.2.1:*****:						
cpe:2.3:a:redhat:libvirt:0.2.2:*****:						
cpe:2.3:a:redhat:libvirt:0.2.3:*****:						
cpe:2.3:a:redhat:libvirt:0.3.0:*****:						
cpe:2.3:a:redhat:libvirt:0.3.1:*****:						
cpe:2.3:a:redhat:libvirt:0.3.2:*****:						
cpe:2.3:a:redhat:libvirt:0.3.3:*****:						

cpe:2.3:a:redhat:libvirt:0.4.0:*****:
cpe:2.3:a:redhat:libvirt:0.4.1:*****:
cpe:2.3:a:redhat:libvirt:0.4.2:*****:
cpe:2.3:a:redhat:libvirt:0.4.3:*****:
cpe:2.3:a:redhat:libvirt:0.4.4:*****:
cpe:2.3:a:redhat:libvirt:0.4.5:*****:
cpe:2.3:a:redhat:libvirt:0.4.6:*****:
cpe:2.3:a:redhat:libvirt:0.5.0:*****:
cpe:2.3:a:redhat:libvirt:0.5.1:*****:
cpe:2.3:a:redhat:libvirt:0.6.0:*****:
cpe:2.3:a:redhat:libvirt:0.6.1:*****:
cpe:2.3:a:redhat:libvirt:0.6.2:*****:
cpe:2.3:a:redhat:libvirt:0.6.3:*****:
cpe:2.3:a:redhat:libvirt:0.6.4:*****:
cpe:2.3:a:redhat:libvirt:0.6.5:*****:
cpe:2.3:a:redhat:libvirt:0.7.0:*****:
cpe:2.3:a:redhat:libvirt:0.7.1:*****:
cpe:2.3:a:redhat:libvirt:0.7.2:*****:
cpe:2.3:a:redhat:libvirt:0.7.3:*****:
cpe:2.3:a:redhat:libvirt:0.7.4:*****:
cpe:2.3:a:redhat:libvirt:0.7.5:*****:
cpe:2.3:a:redhat:libvirt:0.7.6:*****:
cpe:2.3:a:redhat:libvirt:0.7.7:*****:
cpe:2.3:a:redhat:libvirt:0.8.0:*****:
cpe:2.3:a:redhat:libvirt:0.8.1:*****:
cpe:2.3:a:redhat:libvirt:0.8.2:*****:
cpe:2.3:a:redhat:libvirt:0.8.3:*****:
cpe:2.3:a:redhat:libvirt:0.8.4:*****:
cpe:2.3:a:redhat:libvirt:0.8.5:*****:

cpe:2.3:a:redhat:libvirt:0.8.0:*****:
cpe:2.3:a:redhat:libvirt:0.8.6:*****:
cpe:2.3:a:redhat:libvirt:0.8.7:*****:
cpe:2.3:a:redhat:libvirt:0.8.8:*****:
cpe:2.3:a:redhat:libvirt:0.9.0:*****:
cpe:2.3:a:redhat:libvirt:0.9.1:*****:
cpe:2.3:a:redhat:libvirt:*****:
cpe:2.3:a:redhat:libvirt:0.0.1:*****:
cpe:2.3:a:redhat:libvirt:0.0.2:*****:
cpe:2.3:a:redhat:libvirt:0.0.3:*****:
cpe:2.3:a:redhat:libvirt:0.0.4:*****:
cpe:2.3:a:redhat:libvirt:0.0.5:*****:
cpe:2.3:a:redhat:libvirt:0.0.6:*****:
cpe:2.3:a:redhat:libvirt:0.1.0:*****:
cpe:2.3:a:redhat:libvirt:0.1.1:*****:
cpe:2.3:a:redhat:libvirt:0.1.3:*****:
cpe:2.3:a:redhat:libvirt:0.1.4:*****:
cpe:2.3:a:redhat:libvirt:0.1.5:*****:
cpe:2.3:a:redhat:libvirt:0.1.6:*****:
cpe:2.3:a:redhat:libvirt:0.1.7:*****:
cpe:2.3:a:redhat:libvirt:0.1.8:*****:
cpe:2.3:a:redhat:libvirt:0.1.9:*****:
cpe:2.3:a:redhat:libvirt:0.2.0:*****:
cpe:2.3:a:redhat:libvirt:0.2.1:*****:
cpe:2.3:a:redhat:libvirt:0.2.2:*****:
cpe:2.3:a:redhat:libvirt:0.2.3:*****:
cpe:2.3:a:redhat:libvirt:0.3.0:*****:
cpe:2.3:a:redhat:libvirt:0.3.1:*****:
cpe:2.3:a:redhat:libvirt:0.3.2:*****:

cpe:2.3:a:redhat:libvirt:0.3.3:*****:
cpe:2.3:a:redhat:libvirt:0.4.0:*****:
cpe:2.3:a:redhat:libvirt:0.4.1:*****:
cpe:2.3:a:redhat:libvirt:0.4.2:*****:
cpe:2.3:a:redhat:libvirt:0.4.3:*****:
cpe:2.3:a:redhat:libvirt:0.4.4:*****:
cpe:2.3:a:redhat:libvirt:0.4.5:*****:
cpe:2.3:a:redhat:libvirt:0.4.6:*****:
cpe:2.3:a:redhat:libvirt:0.5.0:*****:
cpe:2.3:a:redhat:libvirt:0.5.1:*****:
cpe:2.3:a:redhat:libvirt:0.6.0:*****:
cpe:2.3:a:redhat:libvirt:0.6.1:*****:
cpe:2.3:a:redhat:libvirt:0.6.2:*****:
cpe:2.3:a:redhat:libvirt:0.6.3:*****:
cpe:2.3:a:redhat:libvirt:0.6.4:*****:
cpe:2.3:a:redhat:libvirt:0.6.5:*****:
cpe:2.3:a:redhat:libvirt:0.7.0:*****:
cpe:2.3:a:redhat:libvirt:0.7.1:*****:
cpe:2.3:a:redhat:libvirt:0.7.2:*****:
cpe:2.3:a:redhat:libvirt:0.7.3:*****:
cpe:2.3:a:redhat:libvirt:0.7.4:*****:
cpe:2.3:a:redhat:libvirt:0.7.5:*****:
cpe:2.3:a:redhat:libvirt:0.7.6:*****:
cpe:2.3:a:redhat:libvirt:0.7.7:*****:
cpe:2.3:a:redhat:libvirt:0.8.0:*****:
cpe:2.3:a:redhat:libvirt:0.8.1:*****:
cpe:2.3:a:redhat:libvirt:0.8.2:*****:
cpe:2.3:a:redhat:libvirt:0.8.3:*****:
cpe:2.3:a:redhat:libvirt:0.8.4:*****:

cpe:2.3:a:redhat:libvirt:0.8.4:*****:
cpe:2.3:a:redhat:libvirt:0.8.5:*****:
cpe:2.3:a:redhat:libvirt:0.8.6:*****:
cpe:2.3:a:redhat:libvirt:0.8.7:*****:
cpe:2.3:a:redhat:libvirt:0.8.8:*****:
cpe:2.3:a:redhat:libvirt:0.9.0:*****:
cpe:2.3:a:redhat:libvirt:0.9.1:*****:

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](#)