



# CVE-2011-1750

Published on: 06/21/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:30:00 AM UTC

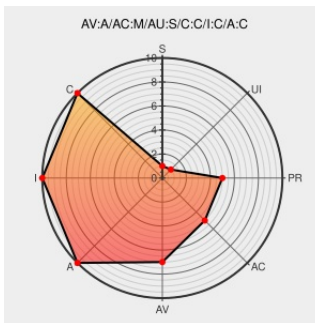
## CVE-2011-1750

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Multiple heap-based buffer overflows in the virtio-blk driver (hw/virtio-blk.c) in qemu-kvm 0.14.0 allow local guest users to cause a denial of service (guest crash) and possibly gain privileges via a (1) write request to the virtio\_blk\_handle\_write function or (2) read request to the virtio\_blk\_handle\_read function that is not properly aligned.

CVE-2011-1750 has been assigned by [secalert@redhat.com](mailto:secalert@redhat.com) to track the vulnerability

CVSS2 Score: **7.4 - HIGH**

Access  
Vector

Access  
Complexity

Authentication

ADJACENT\_NETWORK

MEDIUM

SINGLE

Confidentiality  
Impact

Integrity  
Impact

Availability  
Impact

COMPLETE

COMPLETE

COMPLETE

## CVE References

Description

Tags

Link

Red Hat Customer Portal

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

[MISC access.redhat.com/errata/RHSA-2011:0534](https://access.redhat.com/errata/RHSA-2011:0534)

[Qemu-devel] virtio-blk.c  
handling of i/o which is  
not a 512 multiple

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

[MLIST \[Qemu-devel\] 20110330 virtio-blk.c handling of i/o which is not a 512 multiple](#)

Bug 698906 – CVE-  
2011-1750 virtio-blk:  
heap buffer overflow  
caused by unaligned  
requests

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

[MISC bugzilla.redhat.com/show\\_bug.cgi?id=698906](https://bugzilla.redhat.com/show_bug.cgi?id=698906)

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

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

[REDHAT RHSA-2011:0534](https://access.redhat.com/errata/RHSA-2011:0534)

|                                                                              |                                                                                                                            |                                                                                                                                                                                              |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                              | <a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                                                 |                                                                                                                                                                                              |
| SUSE update for kvm - Secunia.com                                            | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a>                            |  SECUNIA 44660                                                                                              |
| openSUSE-SU-2011:0510-1: moderate: kvm security update                       | <a href="#">lists.opensuse.org</a><br><a href="#">text/html</a>                                                            |  SUSE openSUSE-SU-2011:0510                                                                                 |
| Debian -- Security Information -- DSA-2230-1 qemu-kvm                        | <a href="#">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a>                             |  DEBIAN DSA-2230                                                                                            |
| Red Hat update for qemu-kvm - Secunia.com                                    | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a>                            |  SECUNIA 44658                                                                                              |
| Re: [Qemu-devel] virtio-blk.c handling of i/o which is not a 512 multipl     | <a href="#">lists.gnu.org</a><br><a href="#">text/x-diff</a>                                                               |  MLIST [Qemu-devel] 20110330 Re: virtio-blk.c handling of i/o which is not a 512 multiple                   |
| CVE-2011-1750 - Red Hat Customer Portal                                      | <a href="#">access.redhat.com</a><br><a href="#">text/html</a>                                                             |  MISC access.redhat.com/security/cve/CVE-2011-1750                                                          |
| USN-1145-1: QEMU vulnerabilities   Ubuntu                                    | <a href="#">www.ubuntu.com</a><br><a href="#">text/html</a>                                                                |  UBUNTU USN-1145-1                                                                                          |
| <a href="#">No Description Provided</a>                                      | <a href="#">www.osvdb.org</a>                                                                                              |  OSVDB 73756                                                                                                |
|                                                                              | <a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                                                 |                                                                                                                                                                                              |
| <a href="#">No Description Provided</a>                                      | <a href="#">hermes.opensuse.org</a>                                                                                        |  SUSE SUSE-SU-2011:0533                                                                                   |
|                                                                              | <a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                                                 |                                                                                                                                                                                              |
| KVM qemu-kvm virtio-blk Driver Buffer Overflow Vulnerabilities - Secunia.com | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a>                            |  SECUNIA 44132                                                                                            |
| IBM X-Force Exchange                                                         | <a href="#">exchange.xforce.ibmcloud.com</a><br><a href="#">text/html</a>                                                  |  XF kvm-virtio-blk-priv-escalation(67062)                                                                 |
| [SECURITY] Fedora 15 Update: qemu-0.14.0-9.fc15                              | <a href="#">lists.fedoraproject.org</a><br><a href="#">text/html</a>                                                       |  FEDORA FEDORA-2012-8604                                                                                  |
| Debian update for qemu-kvm - Secunia.com                                     | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a>                            |  SECUNIA 44393                                                                                            |
| kvm/qemu-kvm.git - QEMU modified to work with kvm                            | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  MISC git.kernel.org/?p=virt/kvm/qemu-kvm.git%3Ba=commitdiff%3Bh=52c050236eaa4f0b5e1d160cd66dc18106445c4d |
| Ubuntu update for qemu-kvm - Secunia.com                                     | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a>                            |  SECUNIA 44900                                                                                            |

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](mailto:comment@cve.report).

There are currently no CIDs associated with this CVE

There are currently no CIDs associated with this CVE

| Known Affected Configurations (CPE V2.3) |        |         |         |        |         |          |
|------------------------------------------|--------|---------|---------|--------|---------|----------|
| Type                                     | Vendor | Product | Version | Update | Edition | Language |
| Application                              | Qemu   | Qemu    | 0.14.0  | All    | All     | All      |
| Application                              | Qemu   | Qemu    | 0.14.0  | All    | All     | All      |
| cpe:2.3:a:qemu:qemu:0.14.0:*****:        |        |         |         |        |         |          |
| cpe:2.3:a:qemu:qemu:0.14.0:*****:        |        |         |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→