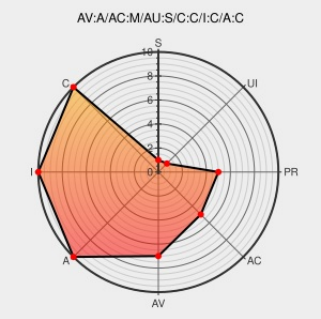
# CVE-2011-1750

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 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 text/html | MISC 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 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 text/html | MISC bugzilla.redhat.com/show_bug.cgi?id=698906 |
| access.redhat.com | web.archive.org text/html | REDHAT RHSA-2011:0534 |

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



There are currently no OIDs associated with this CVE

There are currently no QIDs 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→