

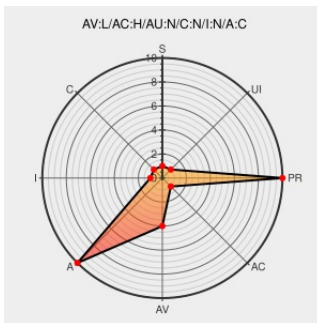


CVE-2011-3346

Published on: 03/31/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:20:00 AM UTC

CVE-2011-3346

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

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

Buffer overflow in hw/scsi-disk.c in the SCSI subsystem in QEMU before 0.15.2, as used by Xen, might allow local guest users with permission to access the CD-ROM to cause a denial of service (guest crash) via a crafted SAI READ CAPACITY SCSI command. NOTE: this is only a vulnerability when root has manually modified certain

permissions or ACLs.

CVE-2011-3346 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
git.qemu.org Git - qemu-stable-0.15.git/log	git.qemu.org text/xml	MISC git.qemu.org/?p=qemu-stable-0.15.git%3Ba=log
Support	www.redhat.com text/html	REDHAT RHSA-2011:1401
oss-security - qemu: CVE-2011-3346	www.openwall.com text/html	MLIST [oss-security] 20111020 qemu: CVE-2011-3346
scsi-disk: lazily allocate bounce buffer · bonzini/qemu@7285477 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/bonzini/qemu/commit/7285477ab11831b1cf56e45878a89170dd06d9b9

Bug 736038 – CVE-2011-3346 qemu: local DoS with SCSI CD-ROM

text/html

 [CONFIRM bugzilla.redhat.com/show_bug.cgi?id=736038](https://bugzilla.redhat.com/show_bug.cgi?id=736038)

scsi-disk: commonize iovec
creation between reads and
writes · [bonzini/qemu@103b40f](https://github.com/bonzini/qemu) ·
GitHub

Patch

text/ht

110

 CONFIRM

github.com/bonzini/gemu/commit/103b40f51e4012b3b0ad20f615562a1806d7f49a

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	Qemu	Qemu	0.15.0	rc1	All	All
Application	Qemu	Qemu	0.15.0	rc2	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	0.15.0	rc1	All	All
Application	Qemu	Qemu	0.15.0	rc2	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Xen	Xen	-	All	All	All
Operating System	Xen	Xen	-	All	All	All

```
cpe:2.3:a:qemu:qemu:0.15.0:rc1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:qemu:qemu:0.15.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:gemu:gemu:*.:*:*:*:*:*:
```

```
cpe:2.3:a:qemu:qemu:0.15.0:rc1:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:qemu:qemu:0.15.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:
```

```
cpe:2.3:o:xen:xen:-:*:*:*:*:*:
```

```
cpe:2.3:o:xen:xen:-:*:*:*:*:*:
```

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](#)