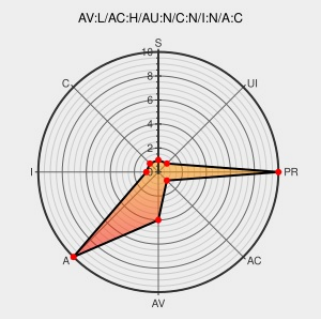
CVE-2011-3346

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	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=736038
scsi-disk: commonize iovec creation between reads and writes · bonzini/qemu@103b40f · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/bonzini/qemu/commit/103b40f51e4012b3b0ad20f615562a1806d7f49a

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:qemu:qemu:*:*:*:*:*:*:*:*:

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→