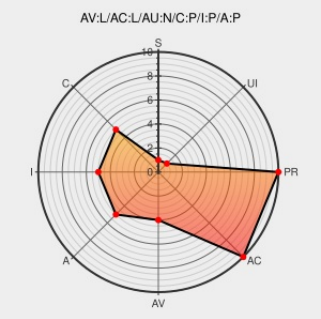
CVE-2014-5388

Published on: 11/15/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:42:00 AM UTC

CVE-2014-5388

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Off-by-one error in the pci_read function in the ACPI PCI hotplug interface (hw/acpi/pcihp.c) in QEMU allows local guest users to obtain sensitive information and have other unspecified impact related to a crafted PCI device that triggers memory corruption.

CVE-2014-5388 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
git.qemu.org Git - qemu.git/commit	Patch, Vendor Advisory, git.qemu.org, text/xml	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=fa365d7cd11185237471823a5a33d36765454e16
oss-sec: CVE request Qemu: out of bounds memory access	Mailing List, Patch, Third Party Advisory, seclists.org, text/html	MLIST [oss-security] 20140822 CVE request Qemu: out of bounds memory access
USN-2409-1: QEMU vulnerabilities | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-2409-1
Bug 1132956 – CVE-2014-5388 Qemu: out of bounds memory	Issue Tracking, Third Party Advisory	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1132956

access	Third Party Advisory bugzilla.redhat.com text/html	
oss-sec: Re: CVE request Qemu: out of bounds memory access	Mailing List Third Party Advisory seclists.org text/html	MLIST [oss-security] 20140822 Re: CVE request Qemu: out of bounds memory access
[Qemu-devel] [PATCH v2] pcihp: fix possible array out of bounds	Patch Third Party Advisory lists.gnu.org text/x-diff	MLIST [Qemu-devel] 20140820 [PATCH v2] pcihp: fix possible array out of bounds

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Application	Qemu	Qemu	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→