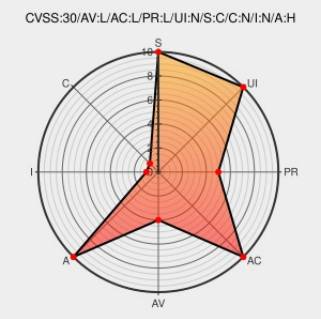
CVE-2016-2392

Published on: 06/16/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:50:00 AM UTC

CVE-2016-2392

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



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

The is_rndis function in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 does not properly validate USB configuration descriptor objects, which allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving a remote NDIS control message packet.

CVE-2016-2392 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 1599-1] qemu security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update

oss-security - CVE request Qemu: usb: null pointer dereference in remote NDIS control message handling	www.openwall.com text/html	MLIST [oss-security] 20160216 CVE request Qemu: usb: null pointer dereference in remote NDIS control message handling
git.qemu.org Git - qemu.git/commit	git.qemu.org text/xml	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=80eecda8e5d09c442c24307f340840a5b70ea3b9
1302299 – (CVE-2016-2392) CVE-2016-2392 Qemu: usb: null pointer dereference in remote NDIS control message handling	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1302299
[Qemu-devel] [PATCH] usb: check USB configuration descriptor object	Vendor Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20160211 [Qemu-devel] [PATCH] usb: check USB configuration descriptor object
USN-2974-1: QEMU vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2974-1
QEMU: Multiple vulnerabilities (GLSA 201604-01) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201604-01
[Qemu-stable] [ANNOUNCE] QEMU 2.5.1 Stable released	Vendor Advisory lists.nongnu.org text/html	MLIST [qemu-stable] 20160329 [Qemu-stable] [ANNOUNCE] QEMU 2.5.1 Stable released
QEMU CVE-2016-2392 Null Pointer Dereference Denial of Service Vulnerability	cve.report (archive) text/html	BID 83274

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	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	15.10	All	All	All

Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Application	Qemu	Qemu	2.5.0	All	All	All
Application	Qemu	Qemu	2.5.0	All	All	All

- cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:a:qemu:qemu:2.5.0:*:*:*:*:*:*:*:
- cpe:2.3:a:qemu:qemu:2.5.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→