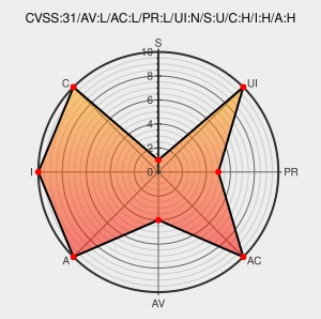
CVE-2016-5338

Published on: 06/14/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:23:00 PM UTC

CVE-2016-5338

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



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

The (1) esp_reg_read and (2) esp_reg_write functions in hw/scsi/esp.c in QEMU allow local guest OS administrators to cause a denial of service (QEMU process crash) or execute arbitrary code on the QEMU host via vectors related to the information transfer buffer.

CVE-2016-5338 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

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
[SECURITY] [DLA 1599-1] qemu security update	Mailing List, Third Party Advisory, lists.debian.org, text/html	MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update

oss-security - Re: CVE Request Qemu: scsi: esp: OOB r/w access while processing ESP_FIFO	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160608 Re: CVE Request Qemu: scsi: esp: OOB r/w access while processing ESP_FIFO
git.qemu.org Git - qemu.git/commit	git.qemu.org text/xml	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=ff589551c8e8e9e95e211b9d8daafb4ed39f1aec
Re: [Qemu-devel] [PATCH v3] scsi: esp: check TI buffer index before read	Mailing List Patch Third Party Advisory lists.gnu.org text/html	MLIST [qemu-devel] 20160606 [Qemu-devel] [PATCH v3] scsi: esp: check TI buffer index before read/write
USN-3047-1: QEMU vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3047-1
QEMU 'hw/scsi/esp.c' Multiple Remote Code Execution Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 91079
oss-security - CVE Request Qemu: scsi: esp: OOB r/w access while processing ESP_FIFO	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160607 CVE Request Qemu: scsi: esp: OOB r/w access while processing ESP_FIFO
USN-3047-2: QEMU regression | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3047-2
QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201609-01

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	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	16.04	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

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:16.04:*:*:*:lts:*:*:*:

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:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→