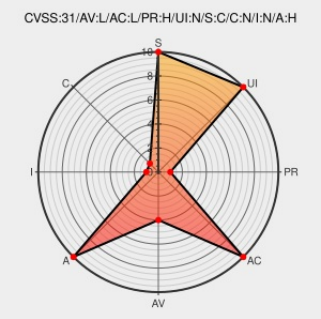
CVE-2016-4441

Published on: 05/20/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:21 AM UTC

CVE-2016-4441

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



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

The get_cmd function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check DMA length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via unspecified vectors, involving an SCSI command.

CVE-2016-4441 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	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	Mailing List, Third Party Advisory, lists.debian.org	MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update

	text/html	
oss-security - CVE-2016-4441 Qemu: scsi: esp: OOB write while writing to 's-cmdbuf' in get_cmd	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160519 CVE-2016-4441 Qemu: scsi: esp: OOB write while writing to 's-cmdbuf' in get_cmd
USN-3047-1: QEMU vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3047-1
1337505 – (CVE-2016-4441) CVE-2016-4441 Qemu: scsi: esp: OOB write while writing to 's->cmdbuf' in get_cmd	Issue Tracking Third Party Advisory VDB Entry bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1337505
USN-3047-2: QEMU regression | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3047-2
[Qemu-devel] [PATCH 2/2] scsi: check dma length before reading scsi comm	Mailing List Patch Third Party Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20160519 [PATCH 2/2] scsi: check dma length before reading scsi command(CVE-2016-4441)
QEMU CVE-2016-4441 Remote Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 90762
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	Canonical	Ubuntu Linux	16.04	All	All	All

System						
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:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:
- 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: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→