CVE-2016-5238

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-5238
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-14 14:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The get_cmd function in hw/scsi/esp.c in QEMU might allow local guest OS administrators to cause a denial of service (out-

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-787 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	2.1		AV:L/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:L/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

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	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Re: [Qemu-devel] [PATCH] scsi: check buffer length before reading scsi c	af854a3a-2127-422b-91
oss-security - Re: CVE Request Qemu: scsi: esp: OOB write when using non-DMA mode in get_cmd	af854a3a-2127-422b-91
[SECURITY] [DLA 1599-1] qemu security update	af854a3a-2127-422b-91
QEMU 'get_cmd()' Function Denial of Service Vulnerability	af854a3a-2127-422b-91
1341931 – (CVE-2016-5238) CVE-2016-5238 Qemu: scsi: esp: OOB write when using non-DMA mode in get_cmd	af854a3a-2127-422b-91
QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security	af854a3a-2127-422b-91

USN-3047-2: QEMU regression | Ubuntu	af854a3a-2127-422b-91
oss-security - CVE Request Qemu: scsi: esp: OOB write when using non-DMA mode in get_cmd	af854a3a-2127-422b-91
[Qemu-devel] [PATCH] scsi: check buffer length before reading scsi comma	af854a3a-2127-422b-91
USN-3047-1: QEMU vulnerabilities | Ubuntu	af854a3a-2127-422b-91
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.