CVE-2016-6351

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

Summary

CVE	CVE-2016-6351
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-07 18:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The esp_do_dma function in hw/scsi/esp.c in QEMU (aka Quick Emulator), when built with ESP/NCR53C9x controller emul

Risk And Classification

Primary CVSS: v3.1 6.7 MEDIUM from nvd@nist.gov

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

EPSS: 0.001670000 probability, percentile 0.374050000 (date 2026-05-06)

Problem Types: NVD-CWE-noinfo | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

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
[SECURITY] [DLA 1599-1] qemu security update	af854a3a-2127-422b-91ae-364da2661108
oss-security - CVE request Qemu: scsi: esp: oob write access while reading ESP command	af854a3a-2127-422b-91ae-364da2661108
oss-security - Re: CVE request Qemu: scsi: esp: oob write access while reading ESP command	af854a3a-2127-422b-91ae-364da2661108
git.qemu.org Git - qemu.git/commit	af854a3a-2127-422b-91ae-364da2661108
git.qemu.org Git - qemu.git/commit	af854a3a-2127-422b-91ae-364da2661108

USN-3047-2: QEMU regression | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
QEMU 'hw/scsi/esp.c' Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da2661108
USN-3047-1: QEMU vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
git.qemu.org Git - qemu.git/commit	MITRE
git.qemu.org Git - qemu.git/commit	MITRE
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.