CVE-2016-2538

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

Summary

CVE	CVE-2016-2538
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-16 18:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple integer overflows in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 allow local guest C

Risk And Classification

Primary CVSS: v3.0 7.1 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Problem Types: CWE-189 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H
2.0	nvd@nist.gov	Primary	3.6		AV:L/AC:L/Au:N/C:P/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
USN-2974-1: QEMU vulnerabilities | Ubuntu	af854a3a-2127-422b-
oss-security - CVE request Qemu: usb: integer overflow in remote NDIS control message handling	af854a3a-2127-422b-
1303120 – (CVE-2016-2538) CVE-2016-2538 Qemu: usb: integer overflow in remote NDIS control message handling	af854a3a-2127-422b-
[Qemu-stable] [ANNOUNCE] QEMU 2.5.1 Stable released	af854a3a-2127-422b-
[SECURITY] [DLA 1599-1] qemu security update	af854a3a-2127-422b-
[Qemu-devel] [PATCH 2/2] usb: check RNDIS buffer offsets & length	af854a3a-2127-422b-
git.qemu.org Git - qemu.git/commit	af854a3a-2127-422b-
QEMU 'usb/dev-network.c' Integer Overflow Vulnerability	af854a3a-2127-422b-
QEMU: Multiple vulnerabilities (GLSA 201604-01) — Gentoo Security	af854a3a-2127-422b-
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.