



CVE-2016-6490

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-6490
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-10 00:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The virtqueue_map_desc function in hw/virtio/virtio.c in QEMU (aka Quick Emulator) allows local guest OS administrators to

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

EPSS: 0.000750000 probability, percentile 0.223780000 (date 2026-05-10)

Problem Types: CWE-120 | 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

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
Application	Qemu	Qemu	2.7.0	rc0	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	Link
git.qemu.org Git - qemu.git/commit	af854a3a-2127-422b-91ae-364da2661108	git.qemu.org
oss-security - Re: CVE Request Qemu: virtio: infinite loop in virtqueue_pop	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org
oss-security - CVE Request Qemu: virtio: infinite loop in virtqueue_pop	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
[Qemu-devel] [PATCH] virtio: check vring descriptor buffer length	af854a3a-2127-422b-91ae-364da2661108	lists.gnu.org
git.qemu.org Git - qemu.git/commit	MITRE	git.qemu.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

CVE Vulnerability Detail

MITRE

MITRE.org

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)