



CVE-2016-10029

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

Summary

CVE	CVE-2016-10029
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-27 22:59:00 UTC
Updated	2023-02-13 04:50:00 UTC
Description	The virtio_gpu_set_scanout function in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows lo

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All

References

Reference
QEMU 'VIRTIO_GPU_CMD_SET_SCANOUT()' Function Out of Bounds Read Denial of Service Vulnerability
oss-security - Re: CVE request Qemu: display: virtio-gpu: out of bounds read in virtio_gpu_set_scanout
git.qemu.org Git - qemu.git/commit
git.qemu.org Git - qemu.git/commit
QEMU Memory Access Error in VIRTIO_GPU_CMD_SET_SCANOUT Command Lets Local Users on a Guest System Cause Denial of Service
git.qemu.org Git - qemu.git/commit
oss-security - CVE request Qemu: display: virtio-gpu: out of bounds read in virtio_gpu_set_scanout
git.qemu.org Git - qemu.git/commit
CVE Program record
NVD vulnerability detail

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](#)