



CVE-2017-9060

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

Summary

CVE	CVE-2017-9060
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-01 16:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	Memory leak in the virtio_gpu_set_scanout function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local g

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
oss-security - CVE-2017-9060 Qemu: virtio-gpu: host memory leakage in Virtio GPU device	MLIST	www.openwall.com	Mailing
git.qemu.org Git - qemu.git/commit	CONFIRM	git.qemu.org	Issue
git.qemu.org Git - qemu.git/commit		git.qemu.org	
Bug 1452597 – CVE-2017-9060 Qemu: virtio-gpu: host memory leakage in Virtio GPU device	MISC	bugzilla.redhat.com	Issue
QEMU 'display/virtio-gpu.c' Denial of Service Vulnerability	BID	www.securityfocus.com	Third P
QEMU: Multiple vulnerabilities (GLSA 201706-03) — Gentoo security	GENTOO	security.gentoo.org	Third P
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710528](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201706-03)

© [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](#).

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