



# CVE-2017-7718

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

## Summary

<b>CVE</b>	CVE-2017-7718
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-20 17:59:00 UTC
<b>Updated</b>	2023-11-07 02:50:00 UTC
<b>Description</b>	hw/display/cirrus_vga_rop.h in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.9.0	rc0	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	2.9.0	rc0	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	Third Party Advisory
git.qemu.org Git - qemu.git/commit		<a href="#">git.qemu-project.org</a>	
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	Third Party Advisory
[SECURITY] [DLA 1497-1] qemu security update	MLIST	<a href="#">lists.debian.org</a>	Third Party Advisory
QEMU 'hw/display/cirrus_vga_rop.h' Multiple Memory Corruption Vulnerabilities	BID	<a href="#">www.securityfocus.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	Third Party Advisory
git.qemu.org Git - qemu.git/commit	CONFIRM	<a href="#">git.qemu-project.org</a>	Issue Tracking, Patch

Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Bug 1443441 – CVE-2017-7718 Qemu: display: cirrus: OOB read access issue	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking, Patch
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
QEMU: Multiple vulnerabilities (GLSA 201706-03) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
oss-security - CVE-2017-7718 Qemu: display: cirrus: OOB read access issue	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing List, Patch, T
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[378183](#) Virtuozzo Linux Security Update for qemu-kvm (VZLSA-2017:1430)

[378194](#) Virtuozzo Linux Security Update for qemu-guest-agent (VZLSA-2017:1206)

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

[900063](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

© [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](https://status.cve.report)