



# CVE-2016-9921

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

## Summary

<b>CVE</b>	CVE-2016-9921
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-23 22:59:00 UTC
<b>Updated</b>	2023-02-13 04:50:00 UTC
<b>Description</b>	Quick emulator (Qemu) built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to a divide by zero issue. It co

## Risk And Classification

**Problem Types:** CWE-369

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	2.8.0	rc0	All	All
Application	Qemu	Qemu	2.8.0	rc1	All	All
Application	Qemu	Qemu	2.8.0	rc2	All	All
Application	Qemu	Qemu	2.8.0	rc0	All	All
Application	Qemu	Qemu	2.8.0	rc1	All	All
Application	Qemu	Qemu	2.8.0	rc2	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8	All	All	All
Application	Redhat	Openstack	8.0	All	All	All

Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

## References

Reference	Source	Link	Tags
oss-security - Re: CVE request Qemu: display: cirrus_vga: a divide by zero in cirrus_do_copy	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailir
QEMU: Multiple vulnerabilities (GLSA 201701-49) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	Third
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	Third
[SECURITY] [DLA 1497-1] qemu security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailir
Bug 1334398 – CVE-2016-9922 Qemu: display: cirrus_vga: a divide by zero in cirrus_do_copy	MISC	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	
CVE-2016-9921 - Red Hat Customer Portal	MISC	<a href="http://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	Third
QEMU Divide By Zero Multiple Denial of Service Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710389](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201701-49)

© 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](http://status.cve.report)