# CVE-2017-2620

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-2620 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2018-07-27 19:29:00 UTC |
| **Updated** | 2023-11-07 02:43:00 UTC |
| **Description** | Quick emulator (QEMU) before 2.8 built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to an out-of-bound |

## Risk And Classification

**Problem Types:** CWE-125 | CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Citrix | Xenserver | 6.0.2 | All | All | All |
| Application | Citrix | Xenserver | 6.2.0 | sp1 | All | All |
| Application | Citrix | Xenserver | 6.5 | sp1 | All | All |
| Application | Citrix | Xenserver | 7.0 | All | All | All |
| Application | Citrix | Xenserver | 7.1 | All | All | All |
| Application | Citrix | Xenserver | 6.0.2 | All | All | All |
| Application | Citrix | Xenserver | 6.2.0 | sp1 | All | All |
| Application | Citrix | Xenserver | 6.5 | sp1 | All | All |
| Application | Citrix | Xenserver | 7.0 | All | All | All |
| Application | Citrix | Xenserver | 7.1 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Application | Redhat | Openstack | 10 | All | All | All |
| Application | Redhat | Openstack | 10.0 | All | All | All |
| Application | Redhat | Openstack | 5.0 | 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 | 10.0 | All | All | All |
| Application | Redhat | Openstack | 5.0 | 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 |
| Operating System | Xen | Xen | 4.7.1 | r1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Xen | Xen | 4.7.1 | r2 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r3 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r4 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r5 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r6 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r7 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r1 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r2 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r3 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r4 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r5 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r6 | All | All |
| Operating System | Xen | Xen | 4.7.1 | r7 | All | All |
| Operating System | Xen | Xen | All | All | All | All |

## References

| Reference |
|---|
| Xen: Privilege Escalation (GLSA 201703-07) — Gentoo security |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Citrix XenServer Multiple Security Updates |
| Qemu CVE-2017-2620 Remote Code Execution Vulnerability |
| Xen Out-of-Bounds Memory Write Error in cirrus_bitblt_cputovideo() Lets Local Administrative Users on a Guest System Gain Elevated Privile |
| [SECURITY] [DLA 1497-1] qemu security update |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| [SECURITY] [DLA 1270-1] xen security update |
| [Qemu-devel] [PATCH] cirrus: add blit_is_unsafe call to cirrus_bitblt_cp |
| Red Hat Customer Portal |
| Red Hat Customer Portal |
| XSA-209 - Xen Security Advisories |
| Red Hat Customer Portal |
| Red Hat Customer Portal |

| |
|---|
| oss-security - CVE-2017-2620 Qemu: display: cirrus: out-of-bounds access issue while in cirrus_bitblt_cputovideo |
| Red Hat Customer Portal |
| QEMU: Multiple vulnerabilities (GLSA 201704-01) — Gentoo Security |
| 1420484 – (CVE-2017-2620, xsa209) CVE-2017-2620 Qemu: display: cirrus: potential arbitrary code execution via cirrus_bitblt_cputovideo |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

| | |
|---|---|
| 378163 | Virtuozzo Linux Security Update for qemu-kvm (VZLSA-2017:0396) |
| 378167 | Virtuozzo Linux Security Update for qemu-kvm (VZLSA-2017:0352) |
| 378279 | Virtuozzo Linux Security Update for kvm-tools (VZLSA-2017:0454) |
| 500813 | Alpine Linux Security Update for xen |
| 501229 | Alpine Linux Security Update for qemu |
| 504556 | Alpine Linux Security Update for xen |
| 505339 | Alpine Linux Security Update for qemu |
| 710464 | Gentoo Linux Xen Privilege Escalation Vulnerability (GLSA 201703-07) |
| 710523 | Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201704-01) |