CVE-2017-2615

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-2615
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-03 01:29:00 UTC
Updated	2023-02-12 23:29:00 UTC
Description	Quick emulator (QEMU) built with the Cirrus CLGD 54xx VGA emulator support is vulnerable to an out-of-bounds access is

Risk And Classification

Problem Types: 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
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	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	All	All	All	All

References

Reference	S
Xen Bug in Cirrus Display Emulation Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker	S
Red Hat Customer Portal	M
Red Hat Customer Portal	F
CVE-2017-2615 - Red Hat Customer Portal	M
Red Hat Customer Portal	F
QEMU 'hw/display/cirrus_vga.c' Remote Code Execution Vulnerability	B
Citrix XenServer Multiple Security Updates	C
Red Hat Customer Portal	M
QEMU: Multiple vulnerabilities (GLSA 201702-28) — Gentoo Security	G
Red Hat Customer Portal	F
[SECURITY] [DLA 1497-1] qemu security update	M
Red Hat Customer Portal	M
Red Hat Customer Portal	M
Red Hat Customer Portal	F
Red Hat Customer Portal	M
Red Hat Customer Portal	M
Red Hat Customer Portal	M
Red Hat Customer Portal	F
Red Hat Customer Portal	F
Red Hat Customer Portal	M
Red Hat Customer Portal	M
Red Hat Customer Portal	F
1418200 – (CVE-2017-2615) CVE-2017-2615 Qemu: display: cirrus: oob access while doing bitblt copy backward mode	C
Red Hat Customer Portal	F
Xen: Multiple vulnerabilities (GLSA 201702-27) — Gentoo Security	G
Red Hat Customer Portal	M

Red Hat Customer Portal	F
Red Hat Customer Portal	F
oss-security - CVE-2017-2615 Qemu: display: cirrus: oob access while doing bitblt copy backward mode	M
Red Hat Customer Portal	F
Bug 1418200 – CVE-2017-2615 Qemu: display: cirrus: oob access while doing bitblt copy backward mode	M
[Qemu-devel] [PATCH v3] cirrus: fix oob access issue (CVE-2017-2615)	M
Red Hat Customer Portal	F
Red Hat Customer Portal	M
Red Hat Customer Portal	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378154 Virtuozzo Linux Security Update for qemu-kvm (VZLSA-2017:0309)
- 378163 Virtuozzo Linux Security Update for qemu-kvm (VZLSA-2017:0396)
- 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
- 710393 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201702-28)
- 710409 Gentoo Linux Xen Multiple Vulnerabilities (GLSA 201702-27)