CVE-2017-7980

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-7980
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-25 14:29:00 UTC
Updated	2021-08-04 17:15:00 UTC
Description	Heap-based buffer overflow in Cirrus CLGD 54xx VGA Emulator in Quick Emulator (Qemu) 2.8 and earlier allows local gue

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Canonical	Ubuntu Linux	17.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Canonical	Ubuntu Linux	17.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	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 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	7.6	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	7.6	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	7.6	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	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	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
Application	Redhat	Virtualization	3.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
RETIRED: Citrix XenServer Multiple Security Vulnerabilities	BID	www.securityfocus.com	Third I
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
Citrix XenServer Multiple Security Updates	CONFIRM	support.citrix.com	Third I
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
Qemu 'hw/display/cirrus_vga.c' Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third I
[SECURITY] [DLA 1497-1] qemu security update	MLIST	lists.debian.org	Mailing
oss-security - CVE-2017-7980 Qemu: display: cirrus: OOB r/w access issues in bitblt routines	MLIST	www.openwall.com	Mailing
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
Bug 1430056 – CVE-2016-9603 Qemu: cirrus: heap buffer overflow via vnc connection	CONFIRM	bugzilla.redhat.com	Issue
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
QEMU: Multiple vulnerabilities (GLSA 201706-03) — Gentoo security	GENTOO	security.gentoo.org	Patch,
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
USN-3289-1: QEMU vulnerabilities | Ubuntu	UBUNTU	ubuntu.com	Third I
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
Red Hat Customer Portal	REDHAT	access.redhat.com	Third I
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

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)