CVE-2016-9603

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-9603
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-27 21:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	A heap buffer overflow flaw was found in QEMU's Cirrus CLGD 54xx VGA emulator's VNC display driver support before 2.9

Risk And Classification

Problem Types: CWE-119

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

References

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
Citrix XenServer Security Update for CVE-2016-9603
Red Hat Customer Portal
1430056 – (CVE-2016-9603) CVE-2016-9603 Qemu: cirrus: heap buffer overflow via vnc connection
[SECURITY] [DLA 1497-1] qemu security update
Red Hat Customer Portal
Red Hat Customer Portal
Xen Qemu Cirrus VGA Heap Overflow Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker
Red Hat Customer Portal
Red Hat Customer Portal
QEMU CVE-2016-9603 Heap Buffer Overflow Vulnerability
Red Hat Customer Portal
[SECURITY] [DLA 1270-1] xen security update
Red Hat Customer Portal
QEMU: Multiple vulnerabilities (GLSA 201706-03) — Gentoo security
Red Hat Customer Portal
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378194 Virtuozzo Linux Security Update for qemu-guest-agent (VZLSA-2017:1206)
- 378234 Virtuozzo Linux Security Update for qemu-kvm (VZLSA-2017:0987)
- 500814 Alpine Linux Security Update for xen
- 504557 Alpine Linux Security Update for xen
- 510417 Alpine Linux Security Update for xen
- 710528 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201706-03)

© 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 registred 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