



CVE-2007-1320

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

Summary

CVE	CVE-2007-1320
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-02 17:19:00 UTC
Updated	2020-12-15 23:52:00 UTC
Description	Multiple heap-based buffer overflows in the cirrus_invalidate_region function in the Cirrus VGA extension in QEMU 0.8.2, a

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Fedoraproject	Fedora	8	All	All	All
Operating System	Fedoraproject	Fedora	9	All	All	All
Operating System	Fedoraproject	Fedora	8	All	All	All
Operating System	Fedoraproject	Fedora	9	All	All	All
Operating System	Fedoraproject	Fedora Core	6	All	All	All
Operating System	Fedoraproject	Fedora Core	6	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Application	Qemu	Qemu	0.8.2	All	All	All
Application	Qemu	Qemu	0.8.2	All	All	All
Operating System	Xen	Xen	-	All	All	All

Operating System	Xen	Xen	-	All	All	All
------------------	-----	-----	---	-----	-----	-----

References

Reference	Source	Link
Fedora update for kvm - Advisories - Secunia	SECUNIA	secunia.com
tavisio.decsystem.org/virtsec.pdf	MISC	tavisio.decsystem.org
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
[SECURITY] Fedora Core 6 Update: xen-3.0.3-12.fc6	FEDORA	www.redhat.com
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
35494	OSVDB	osvdb.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:002	SUSE	lists.opensuse.org
[SECURITY] Fedora 8 Update: kvm-60-6.fc8	FEDORA	www.redhat.com
Debian -- Security Information -- DSA-1384-1 xen-utils	DEBIAN	www.debian.org
Debian update for qemu - Advisories - Secunia	SECUNIA	secunia.com
KVM Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Support / Security / Advisories // MDVSA-2008:162 Mandriva	MANDRIVA	www.mandriva.com
QEMU Various Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Red Hat update for xen - Advisories - Secunia	SECUNIA	secunia.com
Debian update for xen-utils - Advisories - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-1284-1 qemu	DEBIAN	www.debian.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
QEMU Multiple Local Vulnerabilities	BID	www.securityfocus.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Mandriva update for xen - Advisories - Secunia	SECUNIA	secunia.com
[SECURITY] Fedora 9 Update: kvm-65-7.fc9	FEDORA	www.redhat.com
Fedora update for xen - Advisories - Secunia	SECUNIA	secunia.com
Support / Security / Advisories // MDKSA-2007:203 Mandriva	MANDRIVA	www.mandriva.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)