CVE-2012-3515

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-3515
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-23 20:55:00 UTC
Updated	2023-02-13 04:34:00 UTC
Description	Qemu, as used in Xen 4.0, 4.1 and possibly other products, when emulating certain devices with a virtual console backend,

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All

Operating System	Opensuse	Opensuse	12.2	All	All	All
Application	Qemu	Qemu	All	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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Redhat	Virtualization	5.0	All	All	All
Application	Redhat	Virtualization	6.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Redhat	Virtualization	5.0	All	All	All
Application	Redhat	Virtualization	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All

Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All

References

Reference	Source	Link
git.qemu.org Git - qemu-stable-0.15.git/log	MISC	git.qemu.org
Red Hat Customer Portal	MISC	access.redh
Security Advisory SA50860 - Ubuntu update for qemu - Secunia	SECUNIA	secunia.com
Security Advisory SA50530 - Citrix XenServer Denial of Service and Privilege Escalation Vulnerabilities - Secunia	SECUNIA	secunia.com
Xen CVE-2012-3515 Local Privilege Escalation Vulnerability	BID	www.securit
Red Hat Customer Portal	REDHAT	rhn.redhat.c
Debian -- Security Information -- DSA-2543-1 xen-qemu-dm-4.0	DEBIAN	www.debian
[security-announce] SUSE-SU-2012:1135-1: important: Security update for	SUSE	lists.opensu
[security-announce] openSUSE-SU-2012:1174-1: important: Security Update	SUSE	lists.opensu
Red Hat Customer Portal	REDHAT	rhn.redhat.c
Security Advisory SA50632 - SUSE update for qemu - Secunia	SECUNIA	secunia.com
Red Hat Customer Portal	REDHAT	rhn.redhat.c
Red Hat Customer Portal	MISC	access.redh
851252 – (CVE-2012-3515) CVE-2012-3515 qemu: VT100 emulation vulnerability	MISC	bugzilla.redl
[security-announce] SUSE-SU-2012:1320-1: important: Security update for	SUSE	lists.opensu
Red Hat Customer Portal	MISC	access.redh
Debian -- Security Information -- DSA-2545-1 qemu	DEBIAN	www.debian
Red Hat Customer Portal	MISC	access.redh
Red Hat Customer Portal	REDHAT	rhn.redhat.c

Red Hat Customer Portal	MISC	access.redh
[security-announce] SUSE-SU-2012:1162-1: important: Security update for	SUSE	lists.opensu
Security Advisory SA50913 - SUSE update for qemu - Secunia	SECUNIA	secunia.con
openSUSE-SU-2012:1153-1: moderate: kvm	SUSE	lists.opensu
[security-announce] openSUSE-SU-2012:1572-1: important: XEN: security an	SUSE	lists.opensu
[security-announce] SUSE-SU-2012:1202-1: important: Security update for	SUSE	lists.opensu
[security-announce] SUSE-SU-2012:1203-1: important: Security update for	SUSE	lists.opensu
Red Hat Customer Portal	MISC	access.redh
[Xen-announce] Xen Security Advisory 17 (CVE-2012-3515) - Qemu VT100 emulation vulnerability	MLIST	lists.xen.org
Security Advisory SA50528 - Red Hat update for xen - Secunia	SECUNIA	secunia.con
Security Announcements - Xen	CONFIRM	wiki.xen.org
[security-announce] openSUSE-SU-2012:1170-1: important: qemu: Fix buffer	SUSE	lists.opensu
Security Advisory SA51413 - SUSE update for xen - Secunia	SECUNIA	secunia.con
git.qemu.org Git - qemu-stable-0.15.git/log	CONFIRM	git.qemu.org
[security-announce] SUSE-SU-2012:1205-1: important: Security update for	SUSE	lists.opensu
Citrix XenServer Multiple Security Updates	CONFIRM	support.citri
USN-1590-1: QEMU vulnerability | Ubuntu	UBUNTU	www.ubuntu
oss-security - Xen Security Advisory 17 (CVE-2012-3515) - Qemu VT100 emulation vulnerability	MLIST	www.openw
Red Hat Customer Portal	REDHAT	rhn.redhat.c
[security-announce] openSUSE-SU-2012:1172-1: important: Security Update	SUSE	lists.opensu
Security Advisory SA55082 - Gentoo update for xen - Secunia	SECUNIA	secunia.con
CVE-2012-3515 - Red Hat Customer Portal	MISC	access.redh
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	GENTOO	security.ger
[security-announce] openSUSE-SU-2012:1573-1: important: XEN: security an	SUSE	lists.opensu
[security-announce] SUSE-SU-2012:1132-1: important: Security update for	SUSE	lists.opensu
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	GENTOO	security.ger
[security-announce] SUSE-SU-2012:1129-1: important: Security update for	SUSE	lists.opensu
Security Advisory SA50472 - Xen Multiple Denial of Service and Privilege Escalation Vulnerabilities - Secunia	SECUNIA	secunia.con
Security Advisory SA50689 - SUSE update for kvm - Secunia	SECUNIA	secunia.con
Red Hat Customer Portal	REDHAT	rhn.redhat.c
[security-announce] SUSE-SU-2012:1133-1: important: Security update for	SUSE	lists.opensu
CVE Program record	CVE.ORG	www.cve.or
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**