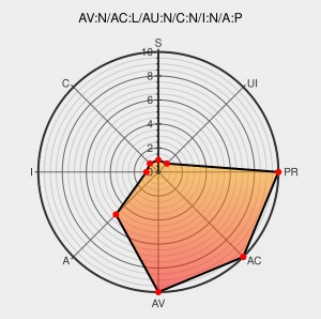
CVE-2014-7815

Published on: 11/14/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:42:00 AM UTC

CVE-2014-7815

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The set_pixel_format function in ui/vnc.c in QEMU allows remote attackers to cause a denial of service (crash) via a small bytes_per_pixel value.

CVE-2014-7815 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Citrix XenServer Multiple Security Updates	Third Party Advisory, support.citrix.com, text/html	CONFIRM support.citrix.com/article/CTX200892
Security Advisory SA62144 - Debian update for qemu - Secunia	Third Party Advisory, web.archive.org, text/html	SECUNIA 62144
Security Advisory SA61484 - QEMU VNC bits_per_pixel Handling Denial of Service Vulnerability - Secunia	Third Party Advisory, web.archive.org, text/html	SECUNIA 61484
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html	REDHAT RHSA-2015:0624

	Inactive Link Not Archived	
[security-announce] SUSE-SU-2015:1782-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2015:1782
git.qemu.org Git - qemu.git/commit	Patch Vendor Advisory git.qemu.org text/xml	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=e6908bfe8e07f2b452e78e677da1b45b1c0f6829
USN-2409-1: QEMU vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2409-1
Debian -- Security Information -- DSA-3066-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3066
Bug 1157641 – CVE-2014-7815 qemu: vnc: insufficient bits_per_pixel from the client sanitization	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1157641
Security Advisory SA62143 - Debian update for qemu-kvm - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 62143
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:0349
Debian -- Security Information -- DSA-3067-1 qemu-kvm	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3067

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating	Canonical	Ubuntu Linux	10.04	All	All	All

Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	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	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	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

System						
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	7.7	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	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:12:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→