CVE-2007-4137

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-4137
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-18 19:17:00 UTC
Updated	2023-11-07 02:00:00 UTC
Description	Off-by-one error in the QUtf8Decoder::toUnicode function in Trolltech Qt 3 allows context-dependent attackers to cause a d

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Conectiva	Linux	10.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Conectiva	Linux	10.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	All	All

Operating System	Mandrakesoft	Mandrake Linux	2007	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	x86_64	All
Operating System	Redhat	Enterprise Linux	2.1	All	as	All
Operating System	Redhat	Enterprise Linux	2.1	All	aw	All
Operating System	Redhat	Enterprise Linux	2.1	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All
Operating System	Redhat	Enterprise Linux	4.0	All	as	All
Operating System	Redhat	Enterprise Linux	4.0	All	es	All
Operating System	Redhat	Enterprise Linux	4.0	All	ws	All
Operating System	Redhat	Enterprise Linux	5.0	All	client	All
Operating System	Redhat	Enterprise Linux	5.0	All	client_workstation	All
Operating System	Redhat	Enterprise Linux	5.0	All	server	All
Operating System	Redhat	Enterprise Linux	2.1	All	as	All
Operating System	Redhat	Enterprise Linux	2.1	All	aw	All
Operating System	Redhat	Enterprise Linux	2.1	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All
Operating System	Redhat	Enterprise Linux	4.0	All	as	All
Operating System	Redhat	Enterprise Linux	4.0	All	es	All
Operating System	Redhat	Enterprise Linux	4.0	All	ws	All
Operating System	Redhat	Enterprise Linux	5.0	All	client	All

Operating System	Redhat	Enterprise Linux	5.0	All	client_workstation	All
Operating System	Redhat	Enterprise Linux	5.0	All	server	All
Operating System	Redhat	Linux	2.1	All	aw_itanium	All
Operating System	Redhat	Linux	3.0	All	All	All
Operating System	Redhat	Linux	4.0	All	All	All
Operating System	Redhat	Linux	2.1	All	aw_itanium	All
Operating System	Redhat	Linux	3.0	All	All	All
Operating System	Redhat	Linux	4.0	All	All	All
Application	Trolltech	Qt	3.0	All	All	All
Application	Trolltech	Qt	3.0.3	All	All	All
Application	Trolltech	Qt	3.0.5	All	All	All
Application	Trolltech	Qt	3.1	All	All	All
Application	Trolltech	Qt	3.1.1	All	All	All
Application	Trolltech	Qt	3.1.2	All	All	All
Application	Trolltech	Qt	3.2.1	All	All	All
Application	Trolltech	Qt	3.2.3	All	All	All
Application	Trolltech	Qt	3.3.0	All	All	All
Application	Trolltech	Qt	3.3.1	All	All	All
Application	Trolltech	Qt	3.3.2	All	All	All
Application	Trolltech	Qt	3.3.3	All	All	All
Application	Trolltech	Qt	3.3.4	All	All	All
Application	Trolltech	Qt	3.3.5	All	All	All
Application	Trolltech	Qt	3.3.6	All	All	All
Application	Trolltech	Qt	3.3.7	All	All	All
Application	Trolltech	Qt	3.3.8	All	All	All
Application	Trolltech	Qt	4.1	All	All	All
Application	Trolltech	Qt	4.1.4	All	All	All
Application	Trolltech	Qt	4.1.5	All	All	All
Application	Trolltech	Qt	4.2	All	All	All
Application	Trolltech	Qt	4.2.1	All	All	All
Application	Trolltech	Qt	4.2.3	All	All	All
Application	Trolltech	Qt	3.0	All	All	All
Application	Trolltech	Qt	3.0.3	All	All	All
Application	Trolltech	Qt	3.0.5	All	All	All
Application	Trolltech	Qt	3.1	All	All	All

Application	Trolltech	Qt	3.1.1	All	All	All
Application	Trolltech	Qt	3.1.2	All	All	All
Application	Trolltech	Qt	3.2.1	All	All	All
Application	Trolltech	Qt	3.2.3	All	All	All
Application	Trolltech	Qt	3.3.0	All	All	All
Application	Trolltech	Qt	3.3.1	All	All	All
Application	Trolltech	Qt	3.3.2	All	All	All
Application	Trolltech	Qt	3.3.3	All	All	All
Application	Trolltech	Qt	3.3.4	All	All	All
Application	Trolltech	Qt	3.3.5	All	All	All
Application	Trolltech	Qt	3.3.6	All	All	All
Application	Trolltech	Qt	3.3.7	All	All	All
Application	Trolltech	Qt	3.3.8	All	All	All
Application	Trolltech	Qt	4.1	All	All	All
Application	Trolltech	Qt	4.1.4	All	All	All
Application	Trolltech	Qt	4.1.5	All	All	All
Application	Trolltech	Qt	4.2	All	All	All
Application	Trolltech	Qt	4.2.1	All	All	All
Application	Trolltech	Qt	4.2.3	All	All	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	amd64	All

Operating System	Ubuntu	Ubuntu Linux	6.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	7.04	All	sparc	All

References

Reference	Source	Link
access.redhat.com | CVE-2007-4137	MISC	access.redhat.com
Trolltech Qt ToUnicode Function Off By One Buffer Overflow Vulnerability	BID	www.securityfocus.cor
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
Fedora update for qt - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
issues.rpath.com/browse/RPL-1751	CONFIRM	issues.rpath.com
dist.trolltech.com/developer/download/175791_4.diff	MISC	dist.trolltech.com
Qt: Buffer overflow — Gentoo Linux Documentation	GENTOO	security.gentoo.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
Webmail- OVH	VUPEN	www.vupen.com
269001 – (CVE-2007-4137) CVE-2007-4137 QT off by one buffer overflow	MISC	bugzilla.redhat.com
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com
rPath update for qt-x11-free - Advisories - Secunia	SECUNIA	secunia.com
Ubuntu update for qt - Advisories - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-1426-1 qt-x11-free	DEBIAN	www.debian.org
Security Announcement	SUSE	www.novell.com
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com
dist.trolltech.com/developer/download/175791_3.diff	MISC	dist.trolltech.com
Debian update for qt-x11-free - Advisories - Secunia	SECUNIA	secunia.com
USN-513-1: Qt vulnerability | Ubuntu	UBUNTU	www.ubuntu.com
Mandriva update for qt - Advisories - Secunia	SECUNIA	secunia.com
Red Hat update for qt - Advisories - Secunia	SECUNIA	secunia.com
Gentoo update for qt - Advisories - Secunia	SECUNIA	secunia.com
404 Not Found	FEDORA	fedoranews.org
Trolltech provides patch to Qt 3 and Qt 4, addressing potential vulnerability — Trolltech	CONFIRM	trolltech.com
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	SECUNIA	secunia.com
Qt QUtf8Decoder Off By One Vulnerability - Advisories - Secunia	SECUNIA	secunia.com

Qt QUtf8Decoder Off-By-One Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Red Hat Customer Portal	MISC	access.redhat.com
20070901-01-P	SGI	patches.sgi.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
Qt Buffer Overflow in QUtf8Decoder May Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	securitytracker.com
Gentoo Bug 192472 - x11-libs/qt convertToUnicode Off-by-one Buffer overflow (CVE-2007-4137)	CONFIRM	bugs.gentoo.org
39384	OSVDB	osvdb.org
Gentoo Linux Documentation -- AMD64 x86 emulation Qt library: Multiple vulnerabilities	GENTOO	security.gentoo.org
Fedora update for qt - Advisories - Secunia	SECUNIA	secunia.com
Avaya Products Qt Overlong UTF-8 Sequence Cross-Site Scripting - Advisories - Secunia	SECUNIA	secunia.com
ASA-2007-424 (RHSA-2007-0883)	CONFIRM	support.avaya.com
Gentoo update for emul-linux-x86-qtlibs - Advisories - Secunia	SECUNIA	secunia.com
404 Not Found	FEDORA	fedoranews.org
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.