CVE-2010-5076

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-5076
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-29 19:55:00 UTC
Updated	2021-06-16 12:43:00 UTC
Description	QSslSocket in Qt before 4.7.0-rc1 recognizes a wildcard IP address in the subject's Common Name field of an X.509 certifi

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digia	Qt	4.0.0	All	All	All
Application	Digia	Qt	4.0.1	All	All	All
Application	Digia	Qt	4.1.0	All	All	All
Application	Digia	Qt	4.1.1	All	All	All
Application	Digia	Qt	4.1.2	All	All	All
Application	Digia	Qt	4.1.3	All	All	All
Application	Digia	Qt	4.1.4	All	All	All
Application	Digia	Qt	4.1.5	All	All	All
Application	Digia	Qt	4.2.0	All	All	All
Application	Digia	Qt	4.2.1	All	All	All
Application	Digia	Qt	4.2.3	All	All	All
Application	Digia	Qt	4.3.0	All	All	All
Application	Digia	Qt	4.3.1	All	All	All
Application	Digia	Qt	4.3.2	All	All	All
Application	Digia	Qt	4.3.3	All	All	All
Application	Digia	Qt	4.3.4	All	All	All
Application	Digia	Qt	4.3.5	All	All	All

Application	Digia	Qt	4.4.0	All	All	All
Application	Digia	Qt	4.4.1	All	All	All
Application	Digia	Qt	4.4.2	All	All	All
Application	Digia	Qt	4.4.3	All	All	All
Application	Digia	Qt	4.5.0	All	All	All
Application	Digia	Qt	4.5.1	All	All	All
Application	Digia	Qt	4.5.2	All	All	All
Application	Digia	Qt	4.5.3	All	All	All
Application	Digia	Qt	4.6.0	All	All	All
Application	Digia	Qt	4.6.0	rc1	All	All
Application	Digia	Qt	4.6.1	All	All	All
Application	Digia	Qt	4.6.2	All	All	All
Application	Digia	Qt	4.6.3	All	All	All
Application	Digia	Qt	4.0.0	All	All	All
Application	Digia	Qt	4.0.1	All	All	All
Application	Digia	Qt	4.1.0	All	All	All
Application	Digia	Qt	4.1.1	All	All	All
Application	Digia	Qt	4.1.2	All	All	All
Application	Digia	Qt	4.1.3	All	All	All
Application	Digia	Qt	4.1.4	All	All	All
Application	Digia	Qt	4.1.5	All	All	All
Application	Digia	Qt	4.2.0	All	All	All
Application	Digia	Qt	4.2.1	All	All	All
Application	Digia	Qt	4.2.3	All	All	All
Application	Digia	Qt	4.3.0	All	All	All
Application	Digia	Qt	4.3.1	All	All	All
Application	Digia	Qt	4.3.2	All	All	All
Application	Digia	Qt	4.3.3	All	All	All
Application	Digia	Qt	4.3.4	All	All	All
Application	Digia	Qt	4.3.5	All	All	All
Application	Digia	Qt	4.4.0	All	All	All
Application	Digia	Qt	4.4.1	All	All	All
Application	Digia	Qt	4.4.2	All	All	All
Application	Digia	Qt	4.4.3	All	All	All
Application	Digia	Qt	4.5.0	All	All	All

Application	Digia	Qt	4.5.1	All	All	All
Application	Digia	Qt	4.5.2	All	All	All
Application	Digia	Qt	4.5.3	All	All	All
Application	Digia	Qt	4.6.0	All	All	All
Application	Digia	Qt	4.6.0	rc1	All	All
Application	Digia	Qt	4.6.1	All	All	All
Application	Digia	Qt	4.6.2	All	All	All
Application	Digia	Qt	4.6.3	All	All	All
Application	Digia	Qt	All	All	All	All
Application	Qt	Qt	4.0.0	All	All	All
Application	Qt	Qt	4.0.1	All	All	All
Application	Qt	Qt	4.1.0	All	All	All
Application	Qt	Qt	4.1.1	All	All	All
Application	Qt	Qt	4.1.2	All	All	All
Application	Qt	Qt	4.1.3	All	All	All
Application	Qt	Qt	4.1.4	All	All	All
Application	Qt	Qt	4.1.5	All	All	All
Application	Qt	Qt	4.2.0	All	All	All
Application	Qt	Qt	4.2.1	All	All	All
Application	Qt	Qt	4.2.3	All	All	All
Application	Qt	Qt	4.3.0	All	All	All
Application	Qt	Qt	4.3.1	All	All	All
Application	Qt	Qt	4.3.2	All	All	All
Application	Qt	Qt	4.3.3	All	All	All
Application	Qt	Qt	4.3.4	All	All	All
Application	Qt	Qt	4.3.5	All	All	All
Application	Qt	Qt	4.4.0	All	All	All
Application	Qt	Qt	4.4.1	All	All	All
Application	Qt	Qt	4.4.2	All	All	All
Application	Qt	Qt	4.4.3	All	All	All
Application	Qt	Qt	4.5.0	All	All	All
Application	Qt	Qt	4.5.1	All	All	All
Application	Qt	Qt	4.5.2	All	All	All
Application	Qt	Qt	4.5.3	All	All	All
Application	Qt	Qt	4.6.0	All	All	All

Application	Qt	Qt	4.6.0	rc1	All	All
Application	Qt	Qt	4.6.1	All	All	All
Application	Qt	Qt	4.6.2	All	All	All
Application	Qt	Qt	4.6.3	All	All	All

References

Reference	Source	Link	Tags
www.westpoint.ltd.uk/advisories/wp-10-0001.txt	MISC	www.westpoint.ltd.uk	
[QTBUG-4455] SSL wildcard verification too broad - Qt Bug Tracker	CONFIRM	bugreports.qt-project.org	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Security Advisory SA49604 - Red Hat update for qt - Secunia	SECUNIA	secunia.com	Vendor Ad
Qt SSL Certificate IP Address Wildcard Matching Vulnerability - Advisories - Community	SECUNIA	secunia.com	Vendor Ad
USN-1504-1: Qt vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com	
qt.gitorious.org/qt/qt/commit/5f6018564668d368f75e431c4cdac88d7421cff0	CONFIRM	qt.gitorious.org	Exploit, Pa
Security Advisory SA49895 - Ubuntu update for qt - Secunia	SECUNIA	secunia.com	Vendor Ad
qt.gitorious.org/qt/qt/commit/846f1b44eea4bb34d080d055badb40a4a13d369e	CONFIRM	qt.gitorious.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

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