



# CVE-2007-5965

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

## Summary

<b>CVE</b>	CVE-2007-5965
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-01-08 01:46:00 UTC
<b>Updated</b>	2011-03-08 03:01:00 UTC
<b>Description</b>	QSSocket in Trolltech Qt 4.3.0 through 4.3.2 does not properly verify SSL certificates, which might make it easier for remote attackers to spoof legitimate SSL certificates and impersonate other hosts.

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Trolltech</a>	<a href="#">Qsslsocket</a>	4.3.0	All	All	All
Application	<a href="#">Trolltech</a>	<a href="#">Qsslsocket</a>	4.3.1	All	All	All
Application	<a href="#">Trolltech</a>	<a href="#">Qsslsocket</a>	4.3.2	All	All	All
Application	<a href="#">Trolltech</a>	<a href="#">Qsslsocket</a>	4.3.0	All	All	All
Application	<a href="#">Trolltech</a>	<a href="#">Qsslsocket</a>	4.3.1	All	All	All
Application	<a href="#">Trolltech</a>	<a href="#">Qsslsocket</a>	4.3.2	All	All	All

## References

Reference	Source	Link
USN-579-1: Qt vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Qt QSSocket Certificate Verification Vulnerability - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Fedora update for qt - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Ubuntu update for qt - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[SECURITY] Fedora 8 Update: qt4-4.3.3-1.fc8	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
Trolltech releases security fix for Qt 4.3 — Trolltech	CONFIRM	<a href="http://trolltech.com">trolltech.com</a>
Support / Security / Advisories // MDVSA-2008:042   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>
Trolltech Qt QSslSocket Class Certificate Verification Security Bypass Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] Fedora 7 Update: qt4-4.3.3-1.fc7	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
Bug 427232 – CVE-2007-5965 qt4: QSslSocket may skip SSL certificate verification	MISC	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-01-08	Mark J Cox	Not vulnerable. This issue did not affect versions of qt or qt4 packages as shipped with Red Hat

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

© [CVE.report](http://CVE.report) 2026 |

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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)