



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 27 avril 2007  
N° CERTA-2007-AVI-159-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Qt

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-159>

---

### Gestion du document

Référence	CERTA-2007-AVI-159-001
Titre	Vulnérabilité dans Qt
Date de la première version	04 avril 2007
Date de la dernière version	27 août 2007
Source(s)	Bulletin de sécurité Trolltech du 03 avril 2007
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Injection de code indirecte (Cross Site Scripting).

## 2 Systèmes affectés

- Qt versions antérieures à 3.3.8 ;
- Qt versions antérieures à 4.2.3.

## 3 Résumé

Une vulnérabilité présente dans Qt permettrait de réaliser des attaques par injection de code indirecte (*Cross Site Scripting*).

## 4 Description

Une vulnérabilité présente dans la fonction de Qt permettant le décodage des chaînes de caractères UTF-8 permettrait à un utilisateur malintentionné de réaliser des attaques par injection de code indirecte (*Cross Site Scripting*) par le biais d'une suite de caractères UTF-8 spécialement conçue.

## 5 Solution

Les versions 3.3.8 et 4.2.3 de Qt corrigent le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Trolltech du 03 avril 2007 :  
<http://www.trolltech.com/company/newsroom/announcements/press.2007-03-30.9172215350>
- Bulletin de sécurité Debian DSA-1292 du 15 mai 2007 :  
<http://www.debian.org/security/2007/dsa-1292>
- Bulletin de sécurité Mandriva MDKSA-2007:074 du 03 avril 2007 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:074>
- Bulletin de sécurité Mandriva MDKSA-2007:075 du 03 avril 2007 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:075>
- Bulletin de sécurité Mandriva MDKSA-2007:076 du 03 avril 2007 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:076>
- Bulletin de sécurité Ubuntu USN-452-1 du 11 avril 2007 :  
<http://www.ubuntu.com/usn/usn-452-1>
- Bulletin de sécurité SuSE SUSE-SR:2007:006 du 13 avril 2007 :  
<http://lists.opensuse.org/opensuse-security-announce/2007-Apr/0002.html>
- Référence CVE CVE-2007-0242 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0242>

## Gestion détaillée du document

**04 avril 2007** version initiale.

**27 août 2007** ajout des références aux bulletins de sécurité de Debian, Mandriva, Ubuntu et SuSE.