

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la bibliothèque graphique 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-2006-AVI-459>

---

### Gestion du document

Référence	CERTA-2006-AVI-459-001
Titre	Vulnérabilité dans la bibliothèque graphique Qt
Date de la première version	20 octobre 2006
Date de la dernière version	25 octobre 2006
Source(s)	Bulletin de sécurité Red Hat RHSA-2006:0720 du 18 octobre 2006
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

## 2 Systèmes affectés

- Qt 3.x ;
- Qt 4.x.

## 3 Résumé

Une vulnérabilité dans la bibliothèque graphique Qt permet à un utilisateur distant mal intentionné de provoquer un déni de service et/ou d'exécuter du code arbitraire à distance.

## 4 Description

La bibliothèque graphique Qt est utilisée par l'environnement graphique KDE.

Une vulnérabilité de type débordement d'entier est causée par une erreur dans le traitement des fichiers image  `pixmap` . Le format  `pixmap`  est essentiellement utilisé dans les icônes des environnements graphiques. Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné afin de provoquer un déni de service et/ou d'exécuter du code arbitraire à distance, au moyen d'un fichier  `pixmap`  spécialement construit.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité RedHat RHSA-2006:0720 du 18 octobre 2006 :  
<http://rhn.redhat.com/errata/RHSA-2006-0720.html>
- Bulletin de sécurité Mandriva MDKSA-2006:186 du 19 octobre 2006 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:186>
- Bulletin de sécurité Ubuntu USN-368-1 du 23 octobre 2006 :  
<http://www.ubuntu.com/usn/usn-368-1>
- Référence CVE CVE-2006-4811 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4811>

## Gestion détaillée du document

**20 octobre 2006** version initiale.

**25 octobre 2006** ajout de la référence au bulletin de sécurité Ubuntu.