Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 septembre 2004
N° CERTA-2004-AVI-275-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque Qt

Gestion du document

Référence	CERTA-2004-AVI-275-002
Titre	Vulnérabilité dans la bibliothèque Qt
Date de la première version	24 août 2004
Date de la dernière version	01 septembre 2004
Source(s)	Bulletin de sécurité Mandrake
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.

2 Systèmes affectés

Bibliothèque Qt versions 3.x antérieures à la version 3.3.3.

3 Résumé

Une vulnérabilité présente dans la bibliothèque `Qt` permet à un utilisateur mal intentionné d'exécuter du code arbitraire ou de réaliser un déni de service.

4 Description

Un débordement de mémoire est présent sur la fonction `read_dib()` utilisée pour le traitement des fichiers `BMP` compressés au format `RLE` 8 bits.

Un utilisateur mal intentionné peut, par le biais d'une image au format `BMP`, exploiter cette vulnérabilité et réaliser un déni de service de l'application qui utilise cette bibliothèque partagée ou exécuter du code arbitraire sur le système.

5 Solution

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

6 Documentation

- Liste des changements de Qt version 3.3.3 :
  http://www.trolltech.com/developer/changes/changes-3.3.3.html
- Bulletin de sécurité de Chris Evans CESA-2004-004 :
  http://scary.beasts.org/security/CESA-2004-004.txt
- Bulletin de sécurité Mandrake MDKSA-2004:085 du 18 août 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:085
- Bulletin de sécurité Suse du 19 août 2004 :
  http://www.suse.de/de/security/2004_27_qt3.html
- Bulletin de sécurité Redhat RHSA-2004:414 du 20 août 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-414.html
- Bulletin de sécurité Gentoo GLSA-200408-20 du 22 août 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200408-20.xml
- Bulletin de sécurité Debian DSA-542 du 30 août 2004 :
  http://www.debian.org/security/2004/dsa-542
- Bulletin de sécurité FreeBSD pour qt du 22 août 2004 :
  http://www.vuxml.org/freebsd/
- Mise à jour de sécurité du paquetage NetBSD qt3-libs :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/qt3-libs/README.html
- Référence CVE CAN-2004-0691 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0691
- Référence CVE CAN-2004-0692 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0692
- Référence CVE CAN-2004-0693 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0693

Gestion détaillée du document

24 août 2004 version initiale.

30 août 2004 ajout des références aux bulletins de sécurité de Chris Evans, FreeBSD et NetBSD ainsi que la liste des changements dans Qt 3.3.3.

01 septembre 2004 ajout de la référence au bulletin de sécurité de Debian.