Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juin 2004
N° CERTA-2004-AVI-168-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sous KDE

Gestion du document

Référence	CERTA-2004-AVI-168-003
Titre	Vulnérabilités sous KDE
Date de la première version	19 mai 2004
Date de la dernière version	15 juin 2004
Source(s)	Avis de sécurité "URI handler vulnerabilities" de KDE. Avis de sécurité MDKSA-2004:047 de Mandrake Avis de sécurité RHSA-2004:222 de Red Hat
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

- Atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Toutes les versions de KDE égales ou antérieures à la version 3.2.2.

3 Résumé

Une vulnérabilité est présente dans le traitement de certains liens (URL) réalisé par KDE.

4 Description

A l'aide de liens (URL) habilement constitués, il est possible de passer des arguments aux applications en charge du traitement de ces liens. Ainsi, en incitant l'utilisateur d'une plate-forme vulnérable à utiliser des liens

astucieusement construits, un utilisateur mal intentionné peut modifier, créer des fichiers avec les droits de la victime sur le système cible.

5 Solution

- Avis de sécurité Mandrake MDKSA-2004:047 du 18 mai 2004 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:047
- Avis de sécurité RedHat RHSA-2004:222 du 17 mai 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-222.html
- Avis de sécurité GLSA 200405-11 de Gentoo du 19 mai 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200405-11.xml
- Bulletin de sécurité SUSE SuSE-SA:2004:014 du 26 mai 2004 :
  http://www.suse.com/de/security/2004_14_kdelibs.html
- Avis de sécurité Debian DSA-518 du 14 juin 2004 :
  http://www.debian.org/security/2004/dsa-518
- Avis de sécurité FreeBSD du 18 mai 2004 :
  http://www.vuxml.org/freebsd/
- Mise à jour de sécurité des paquetages NetBSD kdelibs2 et kdelibs3 :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/kdelibs2/README.html
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/kdelibs3/README.html

6 Documentation

- Avis de sécurité "URI handler vulnerabilities" de KDE :
  http://www.kde.org/info/security/advisory-20040517-1.txt
- Référence CVE CAN-2004-0411 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0411

Gestion détaillée du document

19 mai 2004 version initiale.
24 mai 2004 ajout des références aux bulletins de sécurité Gentoo, FreeBSD et NetBSD.
27 mai 2004 ajout de la référence au bulletin de sécurité SUSE.
15 juin 2004 ajout de la référence au bulletin de sécurité Debian.