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 mars 2005
N° CERTA-2005-AVI-006-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de KDE

Gestion du document

Référence	CERTA-2005-AVI-006-004
Titre	Vulnérabilité de KDE
Date de la première version	05 janvier 2005
Date de la dernière version	01 mars 2005
Source(s)	Bulletin de sécurité de KDE
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

- Usurpation d'identité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

KDE 3.3.2 et version antérieures.

3 Description

KDE est un environnement graphique utilisé sur les systèmes Unix et Linux.

Une vulnérabilité est présente dans le traitement des URL de type `ftp://` rendant possible l'injection de commandes dans une session FTP.

En forcant l'utilisateur d'un programme exploitant le composant KDE `kio_ftp` (tel le navigateur Konqueror) à consulter une URL habilement constituée, il est alors possible de réaliser des attaques par rebond sur certains services réseau (SMTP par exemple).

4 Solution

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

5 Documentation

- Bulletin de sécurité KDE du 01 janvier 2005 :
  http://www.kde.org/info/security/advisory-20050101-1.txt
- Bulletin de sécurité Mandrake MDKSA-2004:160 du 29 décembre 2004 ;
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:160
- Bulletin de sécurité Mandrake MDKSA-2005:045 du 17 février 2005 ;
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:045
- Bulletin de sécurité FreeBSD "kdelibs3 – konqueror FTP command injection vulnerability" du 01 janvier 2005 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Debian DSA-631 du 10 janvier 2005 :
  http://www.debian.org/security/2005/dsa-631
- Bulletin de sécurité Gentoo GLSA 200501-18 du 11 janvier 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200501-18.xml
- Bulletin de sécurité RedHat RHSA-2005:009 du 10 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-009.html
- Bulletin de sécurité RedHat RHSA-2005:065 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-065.html
- Mise à jour de sécurité du paquetage NetBSD kdebase3 :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/kdebase3/README.html
- Référence CVE CAN-2004-1165 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1165

Gestion détaillée du document

05 janvier 2005 version initiale.
11 février 2005 ajout des références aux bulletins de sécurité Debian, Gentoo et RedHat.
17 février 2005 ajout de la référence au bulletin de sécurité RHSA-2005:065 de RedHat.
18 février 2005 ajout de la référence au bulletin de sécurité MDKSA-2005:045 de Mandrake.
01 mars 2005 ajout de la référence au bulletin de sécurité NetBSD.