



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 avril 2005
N° CERTA-2005-AVI-141-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans kdelibs

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-2005-AVI-141>

Gestion du document

Référence	CERTA-2005-AVI-141-002
Titre	Vulnérabilité dans kdelibs
Date de la première version	15 avril 2005
Date de la dernière version	27 mai 2005
Source(s)	Avis SUSE : SUSE-SA:2005:022 Avis Red Hat : RHSA-2005:393-05 Avis Gentoo : GLSA 200504-22/KDE Avis Debian : DSA-174 Avis Mandriva : MDKSA-2005:085

TAB. 1 – *Gestion du document*

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

1 Risque

- Exécution de code arbitraire ;
- nom de domaines homographes ;
- déni de service.

2 Systèmes affectés

- kdelibs3
- Sude 9.1, 9., 9.3
- SUSE Linux Enterprise Server 9
- Novell Linux Desktop 9
- Red Hat Desktop (v.4)
- Red Hat Entreprise Linux AS (v.4)
- Red Hat Entreprise Linux ES (v.4)
- Red Hat Entreprise Linux WS (v.4)

3 Description

Le logiciel KDE offre un environnement graphique de type « bureau » aux utilisateurs des postes de travail Unix. `kdelibs` est l'ensemble des bibliothèques de base nécessaires au fonctionnement d'une application s'appuyant sur l'environnement KDE.

`kdelibs` a fait l'objet de plusieurs publications de vulnérabilités.

3.1 Débordement de variable dans le traitement de certaines images

PCX est un format d'image très populaire dans l'environnement Windows. Un composant de `kdelibs` destiné à manipuler de telles images est vulnérable. Un utilisateur distant mal intentionné peut fabriquer une image au format PCX astucieusement construite. L'ouverture ou la visualisation d'une telle image à l'aide de `kdelibs3` peut conduire à l'exécution de code arbitraire.

3.2 Recouvrement des IDN

IDN désigne les noms de domaine internationaux. Il s'agit de pouvoir donner à des adresses IP des noms de domaine avec des systèmes d'écritures autres que les caractères ASCII traditionnellement utilisés. Il est désormais possible de créer de tels noms de domaine (par exemple « `www.ministère.gouv.fr` » avec le caractère « è » à la place de « `www.ministere.gouv.fr` » avec le caractère « e »).

`kdelibs3` interprète les IDN, ce qui permet les attaques dites par « homographe » : un utilisateur mal intentionné peut acquérir un nom de domaine proche visuellement (la proximité visuelle est obtenue par le fait que de nombreux systèmes d'écriture utilisent des caractères se ressemblant) d'un autre nom de domaine connu. Ce type d'attaque peut être utilisée pour tromper la vigilance de l'internaute dans une démarche de vol d'information de type *phishing* par exemple.

Le correctif de `kdelibs3` n'utilise les homographes que pour les domaines dignes de confiance. La gestion des IDN est désactivée pour les domaines `.com`, `.org` et `.net`.

4 Solution

Les correctifs d'une ou plusieurs de ces vulnérabilités sont couvertes par cet avis. Les correctifs de certaines vulnérabilités sont aussi décrits dans l'avis : CERTA-2005-AVI-101.

5 Documentation

- Explications du problème :
 - La notion d'IDN :
<http://www.afnic.fr/actu/nouvelles/nommage/NN20030217> ;
 - CVE CAN-2005-0237 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0237>
 - CVE CAN-2005-0396 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0396>
 - CVE CAN-2005-1046 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1046>
- Bulletins de sécurité :
 - Bulletin de sécurité Gentoo GLSA 200504-22 / KDE du 22 avril 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200504-22.xml>
 - Bulletin de sécurité Debian DSA-714-1 du 26 avril 2005 :
<http://www.debian.org/security/2005/dsa-714>
 - Bulletin de sécurité Mandriva MDKSA-2005:085 du 12 mai 2005 :
<http://archives.mandrivalinux.com/security-announce/2005-05/msg00006.php>
 - Mise à jour de sécurité pour Fedora Core 2 pour `kdelibs` du 3 mai 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
 - Mise à jour de sécurité pour Fedora Core 3 pour `kdelibs` du 3 mai 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>

- L'avis SUSE :
http://www.novell.com/linux/security/advisories/2005_022_kdelibs3.html
- Mise à jour de sécurité Red Hat :
<http://rhn.redhat.com/errata/RHSA-2005-393.html>

Gestion détaillée du document

15 avril 2005 version initiale.

17 mai 2005 ajout des références aux bulletins de sécurité Gentoo, Debian, Mandriva et Fedora.

27 mai 2005 ajout de références aux bulletins de sécurité Red Hat et au dictionnaire de vulnérabilité CVE.