

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de KDE

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-2004-AVI-406>

Gestion du document

Référence	CERTA-2004-AVI-406
Titre	Vulnérabilité de KDE
Date de la première version	20 décembre 2004
Date de la dernière version	-
Source(s)	Bulletin de sécurité KDE du 12 décembre 2004
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.

2 Systèmes affectés

KDE 3.3.2 et versions antérieures.

3 Description

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

Lors de la création de liens vers des fichiers distants, un partage SAMBA par exemple, les données d'authentification de l'utilisateur sont stockées en clair dans un fichier portant une extension ".desktop".

Si les droits d'accès par défaut aux fichiers de l'utilisateur ne sont pas correctement positionnés (umask), il est alors possible pour un utilisateur local au système de prendre connaissance des mots-de-passe de l'utilisateur.

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 09 décembre 2004 :
<http://www.kde.org/info/security/advisory-20041209-1.txt>
- Bulletin de sécurité Mandrake MDKSA-2004:150 du 15 décembre 2004 ;
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:150>
- Bulletin de sécurité Gentoo GLSA-200412-16 du 19 décembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200412-16.xml>
- Référence CVE CAN-2004-1171 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1171>

Gestion détaillée du document

20 décembre 2004 version initiale.