

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2002-AVI-255>

Gestion du document

Référence	CERTA-2002-AVI-255-001
Titre	Vulnérabilité de kdelibs
Date de la première version	02 décembre 2002
Date de la dernière version	06 décembre 2002
Source(s)	Avis de sécurité KDE Avis de sécurité Mandrake MDKSA-2002:079
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 commandes arbitraires à distance.

2 Systèmes affectés

KDE versions 2.x et 3.x jusqu'aux versions 3.0.4 et 3.1rc3 incluses.

3 Résumé

Une vulnérabilité de la librairie KIO permet à un utilisateur mal intentionné d'exécuter des commandes arbitraires.

4 Description

K Desktop Environment (KDE) fournit une interface pour différents protocoles réseau (HTTP, FTP, POP, SMB,...) via le système KDE Input Output (KIO).

Ce système définit les caractéristiques des protocoles dans des fichiers texte dont l'extension est *.protocol*.

Deux protocoles présentent une vulnérabilité :

- rlogin pour toutes les versions de KDE de 2.1 à 3.0.4 ;
- telnet pour les versions de KDE 2.x.

Ces vulnérabilités permettent à un utilisateur mal intentionné d'exécuter des commandes arbitraires. Ces commandes peuvent être transmises par une URL habilement construite, un mél au format HTML, ou par toute application utilisant KIO.

Les commandes seront exécutées avec les privilèges de la victime.

5 Contournement provisoire

Pour désactiver ces deux protocoles, il suffit de détruire les fichiers *.protocol* correspondants : *telnet.protocol* et *rlogin.protocol*.

Ces fichiers sont normalement installés dans le répertoire */[kdeprefix]/shared/services/*, où [kdeprefix] désigne le répertoire d'installation de KDE.

Des copies de ces fichiers peuvent exister ailleurs, notamment dans le répertoire *.kde/shared/services* des utilisateurs. Il faut également détruire ces copies.

6 Solution

La version 3.0.5 corrige la vulnérabilité.

Vous pouvez appliquer un correctif pour la version 3.0.4 (cf. section Documentation). Pour les autres versions, il est recommandé de mettre à jour à la version 3.0.5.

7 Documentation

Avis de sécurité KDE :

<http://www.kde.org/info/security/advisory-20021111-1.txt>

Avis de sécurité Mandrake MDKSA-2002:079 :

<http://www.mandrakesecure.net/en/advisories/>

Correctif pour la version 3.0.4 de KDE :

ftp://ftp.kde.org/pub/kde/security_patches/

Avis de sécurité Debian DSA-204-1 :

<http://www.debian.org/security/2002/dsa-204>

Gestion détaillée du document

02 décembre 2002 version initiale.

06 décembre 2002 première révision : ajout de l'avis Debian.