

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-2005-AVI-101>

Gestion du document

Référence	CERTA-2005-AVI-101
Titre	Vulnérabilité de KDE
Date de la première version	08 mars 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gento GLSA 200503-14 du 07 mars 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

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

1 Risque

Elévation de privilèges.

2 Systèmes affectés

Version antérieures à KDE 3.3.2-r5.

3 Résumé

Une vulnérabilité découverte dans KDE permet à un utilisateur mal intentionné d'élever localement ses privilèges.

4 Description

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

Le script `dcopidlng` utilisé par KDE est vulnérable à une attaque qui permet l'écrasement de fichiers via le suivi des liens symboliques. A l'aide de liens habilement constitués, un utilisateur mal intentionné, ayant un accès local au système, peut forcer la modification de fichiers avec les droits de la victime.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA 200503-14 / dcofidng du 07 mars 2005 :
<http://www.gentoo.org/security/glsa/glsa-200503-14.xml>
- Référence CVE CAN-2005-0365 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0365>

Gestion détaillée du document

08 mars 2005 version initiale.