



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
*Agence nationale de la sécurité  
des systèmes d'information  
CERTA*

Paris, le 12 mai 2004  
N° CERTA-2004-AVI-007-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans kdepim

---

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-007>

---

### Gestion du document

Référence	CERTA-2004-AVI-007-002
Titre	Vulnérabilité dans kdepim
Date de la première version	15 janvier 2004
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité KDE 20040114-1
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

Elévation de privilèges.

## 2 Systèmes affectés

Toutes les versions de `kdepim` incluses dans KDE en version antérieure à la version 3.1.5.

## 3 Résumé

Une vulnérabilité de `kdepim` dans la gestion des fichiers VCF permet à un utilisateur d'élever ses privilèges.

## 4 Description

`kdepim` (KDE Personal Information Management suite) est un ensemble d'applications permettant la gestion des messages électroniques, des tâches, des rendez-vous et des correspondants. Un débordement de mémoire local dans `kdepim` permet à un utilisateur mal intentionné, construisant habilement un fichier de type VCF, de réaliser une élévation de privilèges et d'exécuter du code arbitraire sur la machine victime.

## 5 Solution

Mettre à jour `kdeplim` selon votre distribution (cf. section documentation).

## 6 Documentation

- Avis de sécurité KDE 20040114-1 :  
<http://www.kde.org/info/security/advisory-20040114-1.txt>
- Avis de sécurité RedHat RHSA-2004:006-04 :  
<http://rhn.redhat.com/errata/RHSA-2004-006.html>
- Avis de sécurité Mandrake MDKSA-2004:003 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:003>
- Avis de sécurité Slackware SSA:2004-014-01 :  
<http://www.slackware.com/lists/archive/viewer.php?l=slackware-security&y=2004&m=slackware-security.442811>
- Avis de sécurité Gentoo GLSA 200404-02 :  
<http://www.gentoo.org/security/en/glsa/glsa-200404-02.xml>
- Avis de sécurité FreeBSD du 15 avril 2004 :  
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2003-0988 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0988>

## Gestion détaillée du document

**15 janvier 2004** version initiale.

**07 avril 2004** ajout du bulletin de sécurité Gentoo.

**12 mai 2004** ajout référence au bulletin de sécurité de FreeBSD.