



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 01 septembre 2004  
N° CERTA-2004-AVI-288

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-288>

---

### Gestion du document

Référence	CERTA-2004-AVI-288
Titre	Multiples vulnérabilités dans KDE
Date de la première version	01 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité
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

- Usurpations ;
- contournement de la politique de sécurité ;
- déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

KDE version 3.2.3 et versions antérieures.

## 3 Description

De multiples vulnérabilités dans KDE permettent à un utilisateur mal intentionné d'usurper des frames, domaines..., de contourner la politique de sécurité, de créer des dénis de service ou d'exécuter du code arbitraire à distance.

## 4 Solution

- Mettre à jour KDE en version 3.3 ;
- des correctifs pour KDE 3.0.5b, 3.1.5 et 3.2.3 sont disponibles à l'adresse suivante :  
[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches)
- selon sa distribution, se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Site Internet de KDE :  
<http://www.kde.org>
- Bulletins de sécurité KDE du 11 août 2004 :  
<http://www.kde.org/info/security/advisory-20040811-1.txt>  
<http://www.kde.org/info/security/advisory-20040811-2.txt>  
<http://www.kde.org/info/security/advisory-20040811-3.txt>
- Bulletin de sécurité KDE du 23 août 2004 :  
<http://www.kde.org/info/security/advisory-20040823-1.txt>
- Bulletin de sécurité Gentoo GLSA 200408-13 pour kde, kdebase et kdelibs du 12 août 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200408-13.xml>
- Bulletin de sécurité Gentoo GLSA 200408-23 pour kde, kdebase et kdelibs du 24 août 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200408-23.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:086 du 20 août 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:086>
- Bulletin de sécurité FreeBSD pour kdelibs du 12 août 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité FreeBSD pour KDE Konqueror du 12 août 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité FreeBSD pour kdelibs du 26 août 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour kdelibs du 25 août 2004 :  
<http://www.vuxml.org/openbsd/>
- Mise à jour de sécurité du paquetage NetBSD kdelibs3 :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/kdelibs3/README.html>
- Mise à jour de sécurité du paquetage NetBSD kdebase3 :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/kdebase3/README.html>
- Référence CVE CAN-2004-0689 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0689>
- Référence CVE CAN-2004-0690 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0690>
- Référence CVE CAN-2004-0721 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0721>
- Référence CVE CAN-2004-0746 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0746>

## Gestion détaillée du document

01 septembre 2004 version initiale.