



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 janvier 2006
N° CERTA-2006-AVI-039-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2006-AVI-039>

Gestion du document

Référence	CERTA-2006-AVI-039-001
Titre	Vulnérabilité dans KDE
Date de la première version	20 janvier 2006
Date de la dernière version	23 janvier 2006
Source(s)	Bulletin de sécurité RedHat RHSA-2006:0184 du 19 janvier 2006
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 code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

KDE 3.x.

3 Résumé

Une vulnérabilité dans KDE permet à un utilisateur mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

La vulnérabilité de type débordement de mémoire est causée par une erreur dans le moteur JavaScript de KDE (kjs).

Un utilisateur mal intentionné peut exploiter cette vulnérabilité, au moyen d'un code JavaScript malicieusement construit qui sera ensuite ouvert par une application mettant en œuvre le moteur JavaScript kjs.

5 Solution

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

6 Documentation

- Bulletin de sécurité KDE du 19 janvier 2006 :
<http://www.kde.org/info/security/advisory-20060119-1.txt>
- Bulletin de sécurité RedHat RHSA-2006:0184 du 19 janvier 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0184.html>
- Bulletin de sécurité Debian DSA-948 du 20 janvier 2006 :
<http://www.debian.org/security/2006/dsa-948>
- Bulletin de sécurité SUSE SUSE-SA:2006:003 du 20 janvier 2006 :
http://www.novell.com/linux/security/advisories/2006_03_kdelibs3.html
- Bulletin de sécurité Mandriva MDKSA-2006:019 du 20 janvier 2006 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:019>
- Bulletin de sécurité Gentoo GLSA-200601-11 du 22 janvier 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200601-11.xml>
- Référence CVE CAN-2006-0019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0019>

Gestion détaillée du document

20 janvier 2006 version initiale.

23 janvier 2006 ajout des références aux bulletins de sécurité KDE, Mandriva et Gentoo.