

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Contournement des règles de sécurité dans Konqueror

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-207>

Gestion du document

Référence	CERTA-2002-AVI-207-001
Titre	Contournement des règles de sécurité dans Konqueror
Date de la première version	13 septembre 2002
Date de la dernière version	17 septembre 2002
Source(s)	Avis #20020908-2 de KDE
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

- Déni de service ;
- Divulgateion de données.

2 Systèmes affectés

Tout système possédant KDE en version 2.2.2, 3.0 à 3.0.3 est vulnérable.

3 Résumé

Les protections de konqueror contre l'exécution du javascript pour certains domaines ne fonctionnent pas dans les sous-cadres de pages (sub-frames).

4 Description

Le code javascript peut s'exécuter, sans le contrôle de Konqueror, dans les sous-cadres de pages (sub-frames) et donc permet une attaque de type « Cross Site Scripting ».

5 Contournement provisoire

Désactiver l'emploi des javascripts.

6 Solution

Appliquer le correctif disponible en téléchargement sur le site de KDE (consulter la section documentation) ou installer la version 3.0.3a de `kdelibs`.

7 Documentation

Bulletin de sécurité #20020908-2 de KDE :
<http://www.kde.org/info/security/advisory-20020908-2.txt>

Page de téléchargement des correctifs :
ftp://ftp.kde.org/pub/kde/security_patches/

Téléchargement de KDE :
<http://download.kde.org/stable/3.0.3/>

Avis #DSA-167 de Dedian :
<http://www.debian.org/security/2002/dsa-167>

Gestion détaillée du document

13 septembre 2002 version initiale ;

17 septembre 2002 ajout de l'avis debian.