

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des cookies sécurisés 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-2002-AVI-208>

Gestion du document

Référence	CERTA-2002-AVI-208
Titre	Vulnérabilité des cookies sécurisés dans KDE
Date de la première version	13 septembre 2002
Date de la dernière version	–
Source(s)	Avis #20020908-1 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

- Divulgence de données ;
- Vol de session.

2 Systèmes affectés

Tout système utilisant Konqueror en version 3.0, 3.0.1 ou 3.0.2 de KDE est vulnérable.
Les versions 2.2.2 et 3.0.3 de KDE ne sont pas vulnérables.

3 Résumé

Konqueror ne détecte pas le drapeau "secure" dans un cookie HTTP. Il transmet donc ces cookies en clair sur le réseau.

4 Description

Les sites internet qui se basent uniquement sur un cookie pour l'identification de la session HTTP peuvent permettre à un utilisateur mal intentionné de récupérer cette session, car le cookie n'est pas chiffré avant son transfert.

Cette vulnérabilité peut aussi être utilisée pour se connecter sur un site se basant uniquement sur un cookie pour l'identification de l'utilisateur.

5 Solution

Mettre KDE à jour.

Les mises à jour sont disponibles en téléchargement sur le site de KDE (Consultez la section Documentation).

6 Documentation

Avis #20020908-1 de KDE :

<http://www.kde.org/info/security/advisory-20020908-1.txt>

Page de téléchargement des mises à jour :

ftp://ftp.kde.org/pub/kde/security_patches/

Gestion détaillée du document

13 septembre 2002 version initiale.