Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mars 2004
N° CERTA-2004-AVI-081

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du navigateur Konqueror

Gestion du document

Référence	CERTA-2004-AVI-081
Titre	Vulnérabilité du navigateur Konqueror
Date de la première version	11 mars 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Corsaire
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

- Divulgation de données ;
- vol de session.

2 Systèmes affectés

Tout système utilisant KDE dans une version antérieure à la 3.1.3.

3 Résumé

Une vulnérabilité dans la gestion des cookies permet à un utilisateur mal intentionné d'accéder à certains d'entre eux sans en avoir les droits.

4 Description

KDE est un environnement graphique pour système Unix, incluant en particulier un navigateur, Konqueror.
Une faille existe au sein des bibliothèques de KDE dans la gestion des cookies.

Un cookie peut comporter un champ qui restreint l'accès au cookie à une sous-arborescence spécifiée d'un site. Hors cette restriction peut être contournée. Lorsque le cookie est utilisé pour l'authentification, un utilisateur mal intentionné, contrôlant des pages sur le même serveur que la zone protégée, peut dérober cet authentifiant à l'aide d'une page HTML habilement construite. Cette faille peut également affecter les clients de messagerie KDE capables d'afficher du HTML.

5 Solution

Mettre à jour KDE en version 3.1.3.

- Red Hat Linux 9 :
  https://rhn.redhat.com/errata/RHSA-2004-075.html
- Linux Mandrake 9.1 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:022
- Debian Linux 3.0 :
  http://www.debian.org/security/2004/dsa-459

6 Documentation

Avis de sécurité de la société Corsaire :
http://www.corsaire.com/advisories/c030712-001.txt

Gestion détaillée du document

11 mars 2004 version initiale.