



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 décembre 2004
N° CERTA-2004-AVI-413-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2004-AVI-413>

Gestion du document

Référence	CERTA-2004-AVI-413-001
Titre	Multiples vulnérabilité dans Konqueror
Date de la première version	22 décembre 2004
Date de la dernière version	23 décembre 2004
Source(s)	Bulletins de sécurité KDE du 13 et du 20 décembre 2004
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

- Elévation de privilèges ;
- Atteinte à la confidentialité de données.

2 Systèmes affectés

Les versions de KDE 3.3.2 et antérieures sont vulnérables.

3 Description

KDE est un environnement graphique pour système Unix et Linux, incluant en particulier Konqueror, gestionnaire de fichiers permettant la navigation sur le web.

Deux failles ont été découvertes dans Konqueror.

La première faille (CAN-2004-1158) permet à un site web de charger une page dans une fenêtre qui était déjà utilisée par un autre site web. La confusion résultant de cette manipulation peut entraîner un utilisateur à envoyer des données confidentielles sur un serveur malicieusement construit, alors qu'il croit les envoyer sur un serveur de confiance.

La deuxième faille (CAN-2004-1145) concerne la gestion de l'environnement d'exécution Java par Konqueror et permet à un utilisateur mal intentionné, via un site web malicieusement construit, d'avoir accès en lecture et en écriture aux fichiers de la victime, avec les droits de l'utilisateur.

4 Solution

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

5 Documentation

- Bulletin de sécurité KDE du 13 décembre 2004
<http://www.kde.org/info/security/advisory-20041213-1.txt>
- Bulletin de sécurité KDE du 20 décembre 2004
<http://www.kde.org/info/security/advisory-20041220-1.txt>
- Avis du CERTA : CERTA-2004-AVI-406
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-406/index.html>
- Bulletin de sécurité Mandrake MDKSA-2004:154 du 22 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:154>
- Référence CVE CAN-2004-1145
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1145>
- Référence CVE CAN-2004-1158
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1158>

Gestion détaillée du document

22 décembre 2004 version initiale.

23 décembre 2004 ajout référence au bulletin de sécurité Mandrake MDKSA-2004:154.