



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2002
N° CERTA-2002-AVI-203-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des certificats SSL 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-203>

Gestion du document

Référence	CERTA-2002-AVI-203-002
Titre	Vulnérabilité des certificats SSL dans KDE
Date de la première version	06 septembre 2002
Date de la dernière version	13 septembre 2002
Source(s)	Avis #20020818-1 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

Usurpation d'identité.

2 Systèmes affectés

Toutes les versions de KDE jusqu'à la version 3.0.2 incluse sont vulnérables.

3 Résumé

KDE ne vérifie pas tous les champs des certificats utilisés pour authentifier des pages Web ou pour signer des méls. Un utilisateur mal intentionné peut générer son propre certificat permettant une usurpation d'identité (attaque de type « man in the middle »).

4 Description

Les certificats au standard X.509 possèdent plusieurs champs d'options. Un de ces champs s'appelle « Basic Constraints Field » et indique la longueur maximum autorisée pour une chaîne de certificats ainsi que si le

certificat est d'autorité ou non. Les bibliothèques de KDE ne vérifient pas ce champ et donc, un certificat, habilement conçu par un utilisateur mal intentionné, peut passer pour un certificat d'autorité.

5 Solution

- Installer la version 3.0.3 des bibliothèques de KDE (kdelibs3.0.3) ;
- Un correctif est disponible pour kde 2.2.2 (Consulter la section Documentation).

6 Documentation

Avis #20020818-1 de KDE :
<http://www.kde.org/info/security/advisory-20020818-1.txt>

Correctif pour la version 2.2.2 de KDE :
ftp://ftp.kde.org/pub/kde/security_patches/

Bulletin de sécurité #DSA-155 de Debian :
<http://www.debian.org/security/2002/dsa-155>

Bulletin de sécurité #MDKSA-2002:058 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-058.php>

Gestion détaillée du document

06 septembre 2002 version initiale ;

09 septembre 2002 Ajout du bulletin de sécurité de Debian ;

13 septembre 2002 Ajout du bulletin de sécurité de Mandrake.