Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 janvier 2003
N° CERTA-2003-AVI-017

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de KCMS sous Solaris

Gestion du document

Référence	CERTA-2003-AVI-017
Titre	Vulnérabilité de KCMS sous Solaris
Date de la première version	29 janvier 2003
Date de la dernière version	–
Source(s)	Bulletin d'alerte #50104 de Sun Note de vulnérabilité VU#850785 du CERT/CC
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

Accès non-autorisé à des données.

2 Systèmes affectés

- Solaris 2.6 sur SPARC et Intel ;
- Solaris 7 sur SPARC et Intel ;
- Solaris 8 sur SPARC et Intel ;
- Solaris 9 sur SPARC et Intel.

3 Résumé

Une vulnérabilité du serveur KCMS permet à un utilisateur mal intentionné de visualiser des fichiers appartenant à l'administrateur `root`.

4 Description

KCMS (*Kodak Color Management System*) est un ensemble d'outils de gestion des profils de couleur des différents périphériques (scanner, imprimante, écran, etc.).

Le service `kcms_server` est installé sur Solaris et lancé par défaut par `inetd`, et permet d'accéder à distance à ces outils.

Une vulnérabilité de `kcms_server` permet à un utilisateur mal intentionné de visualiser des fichiers appartenant à l'administrateur `root` en étant connecté localement ou bien à distance.

5 Contournement provisoire

Désactiver le service `kcms_server`, s'il n'est pas utilisé, en éditant le fichier `inetd.conf`

6 Solution

Se référer au bulletin d'alerte #50104 de Sun (voir paragraphe Documentation) pour connaître la disponibilité des correctifs.

7 Documentation

- Bulletin d'alerte #50104 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50104
- Note de vulnérabilité VU#850785 du CERT/CC :
  http://www.kb.cert.org/vuls/id/850785

Gestion détaillée du document

29 janvier 2003 version initiale.