

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de cachefsds sous Solaris

---

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-091>

---

### Gestion du document

Référence	CERTA-2002-AVI-091
Titre	Multiples vulnérabilités de cachefsds sous Solaris
Date de la première version	02 mai 2002
Date de la dernière version	–
Source(s)	bulletin d'alerte #44309 de Sun
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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Pour les architectures Intel et Sparc, les systèmes suivants sont affectés :

- Solaris 2.5.1 ;
- Solaris 2.6 ;
- Solaris 7 ;
- Solaris 8.

## 3 Résumé

Deux vulnérabilités du *daemon* *cachefsds* ont été mises en évidence :

- Il est possible d'arrêter à distance le *daemon* *cachefsds* ;

- un utilisateur mal intentionné peut exécuter du code arbitraire à distance, avec les privilèges de l'administrateur `root`.

## 4 Description

Le *daemon* `cached` permet la mise en cache localement de données présentes sur un système de fichiers distant.

Un utilisateur mal intentionné peut :

- arrêter le *daemon* à distance au moyen d'une requête contenant un appel de procédure astucieusement construit ;
- obtenir les privilèges de l'administrateur `root` à distance ou localement en effectuant un débordement de mémoire du *daemon* `cached`.

## 5 Contournement provisoire

- Bloquer le port 111/TCP (SUNRPC) au niveau du garde-barrière pour se protéger contre les attaques provenant de l'extérieur.
- Désactiver le service `cached` en commentant comme suit la ligne concernant `cached` dans `/etc/inetd.conf` :  
`#100235/1 tli rpc/tcp wait root /usr/lib/fs/cached/cached`  
et en arrêtant le *daemon* par la commande `kill -HUP`.

## 6 Solution

Se référer au bulletin de Sun pour connaître la disponibilité des correctifs.

## 7 Documentation

Bulletin d'alerte #44309 de Sun :

<http://sunsolve.sun.com/pub-cgi/retrieve.pls?doc=fsalert%2F44309>

## Gestion détaillée du document

**02 mai 2002** version initiale.