

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de 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-2000-AVI-092>

---

### Gestion du document

Référence	CERTA-2000-AVI-092
Titre	Vulnérabilités de Solaris
Date de la première version	20 décembre 2000
Date de la dernière version	–
Source(s)	Sun Microsystems
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

- Augmentation de privilèges ;
- exécution de code avec les privilèges de `root`.

## 2 Systèmes affectés

Sun Solaris 2.x (SunOS 5.x)

## 3 Résumé

`patchadd` et `patchrm` sont des outils qui permettent respectivement d'installer ou de désinstaller des correctifs ou mises à jour du système Solaris de Sun.

Une vulnérabilité de ces outils permet à un utilisateur mal intentionné d'augmenter ses privilèges et d'exécuter localement du code avec les privilèges de `root`.

## 4 Description

`patchadd` et `patchrm` sont des utilitaires qui nécessitent d'être `root` pour être exécutés.

Une mauvaise gestion des fichiers temporaires par ces outils lors d'une mise à jour ou de l'installation d'un correctif permet à un utilisateur mal intentionné d'utiliser ces fichiers temporaires pour obtenir les privilèges de `root` ou bien exécuter du code avec ces privilèges.

## 5 Contournement provisoire

Avant l'installation de correctifs ou de mises à jour, il faut vérifier que le répertoire `/tmp` est vide.

Afin d'être sûr d'être la seule personne connectée, vous pouvez en plus, redémarrer la machine en mode *single user* pour appliquer le correctif ou la mise à jour.

## 6 Solution

Appliquer le correctif proposé par Sun en se plaçant dans les conditions indiquées dans le paragraphe *Contournement provisoire* :

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

## 7 Documentation

Informations indiquées sur la page de téléchargement du correctif :

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

## Gestion détaillée du document

20 décembre 2000 version initiale.