



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2003
N° CERTA-2003-ALE-005

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de sadmind sur 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-2003-ALE-005>

Gestion du document

Référence	CERTA-2003-ALE-005
Titre	Vulnérabilité de sadmind sur Solaris
Date de la première version	19 septembre 2003
Date de la dernière version	–
Source(s)	Avis de sécurité 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

Exécution de code arbitraire.

2 Systèmes affectés

- Solaris versions 7, 8, 9 sur plate-formes sparc et x86 ;
- Trusted Solaris versions 7, 8, 9 sur plate-formes sparc et x86.

3 Résumé

Une vulnérabilité présente sur le service sadmind permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur le système.

4 Description

Le service sadmind est utilisé par la suite Solstice AdminSuite qui est un ensemble d'outils utilisé pour l'administration de système distant.

Une vulnérabilité sur une méthode d'authentification RPC utilisée par `Solstice AdminSuite (AUTH_SYS)` permet à un utilisateur mal intentionné, par le biais de paquets malicieusement construits, d'exécuter du code arbitraire avec les privilèges du super utilisateur (`root`).

Des programmes exploitant cette vulnérabilité sont diffusés sur l'Internet.

5 Contournement provisoire

Si le service n'est pas utilisé : désactiver le service en commentant la ligne suivante dans le fichier `/etc/inetd.conf` :

```
100232 tli rpc/udp wait root /usr/sbin/sadmind
```

Sinon activer l'option d'authentification (`AUTH_DES`) en incluant la ligne suivante dans le fichier `/etc/inetd.conf` (Cette option nécessite l'emploi du service NIS ou NIS+) :

```
100232 tli rpd/udp wait root /usr/sbin/sadmind -S 2
```

6 Solution

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

7 Documentation

- Bulletin de sécurité Sun #56740 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-56740-1>
- Avis de sécurité iDefense :
<http://www.idefense.com/advisory/09.16.03.txt>

Gestion détaillée du document

19 septembre 2003 version initiale.