

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité du service *sadmind* de Sun 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-2008-ALE-013>

---

### Gestion du document

Référence	CERTA-2008-ALE-013
Titre	Vulnérabilité du service <i>sadmind</i> de Sun Solaris
Date de la première version	17 octobre 2008
Date de la dernière version	–
Source(s)	Annonce Bugtraq BUGTRAQ:20081014 [RISE-2008001] du 14 octobre 2008
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 à distance.

## 2 Systèmes affectés

- Sun Solaris 8 pour architecture SPARC ;
- Sun Solaris 8 pour architecture x86 ;
- Sun Solaris 9 pour architecture SPARC ;
- Sun Solaris 9 pour architecture x86.

## 3 Résumé

Une vulnérabilité dans le service *sadmind* de Sun Solaris permet à un utilisateur distant d'exécuter du code arbitraire.

## 4 Description

Le service *sadmind* sur Sun Solaris permet l'administration de systèmes à distance via la suite d'outils Solstice AdminSuite.

Ce service est activé par défaut sous Solaris et est mis en œuvre par le biais du « super-service » *inetd* fonctionnant avec les privilèges de l'administrateur *root*.

Une erreur de type débordement de mémoire présente dans *sadmind* permet à un utilisateur malintentionné distant d'exécuter du code arbitraire sur le système vulnérable.

## 5 Contournement provisoire

Dans la mesure où l'exécution du service *sadmind* est contrôlée par le « super-service » *inetd*, il est possible de le désactiver en mettant en commentaire la ligne suivante dans le fichier */etc/inetd.conf* :

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

Une fois cette ligne commentée, il faudra également demander au service *inetd* de relire sa configuration en tapant la commande :

```
pkill -HUP inetd
```

Si, toutefois, ce service devait être utilisé et ne pouvait être désactivé, il conviendrait d'en limiter l'accès aux seules machines de confiance nécessaires à l'administration.

## 6 Documentation

- Annonce Bugtraq BUGTRAQ:20081014 [RISE-2008001] du 14 octobre 2008 :  
<http://www.securityfocus.com/archive/1/archive/1/497311/100/0/threaded>
- Référence CVE CVE-2008-4556 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4556>

## Gestion détaillée du document

17 octobre 2008 version initiale.