



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 03 juin 2002  
N° CERTA-2002-AVI-096-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de `rpc.rwalld` 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-096>

---

### Gestion du document

Référence	CERTA-2002-AVI-096-001
Titre	Vulnérabilité de <code>rpc.rwalld</code> sous Solaris
Date de la première version	07 mai 2002
Date de la dernière version	03 juin 2002
Source(s)	Avis CA-2002-10 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

Exécution de code arbitraire.

## 2 Systèmes affectés

Sun Solaris 2.5.1, 2.6, 2.7 et 2.8.

## 3 Résumé

Une vulnérabilité du service `rpc.rwalld` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

Le démon `rpc.rwalld` est un serveur en écoute sur le réseau des requêtes `wall`. Lorsqu'il reçoit une telle requête, il appelle la fonction `wall` qui a pour but d'envoyer un message à tous les terminaux du système.

Une vulnérabilité présente dans le code d'affichage des messages d'erreur du démon `rwallld` permet à un utilisateur mal intentionné, sous certaines conditions, d'exécuter du code arbitraire avec les droits du démon `rwallld` (souvent ceux de l'administrateur).

## 5 Contournement provisoire

- Désactiver le service `rpc.rwallld` dans le fichier `/etc/inetd.conf` si celui-ci n'est pas indispensable.
- Filtrer le port `32777/udp` et le port `111/tcp` au niveau du garde-barrière.

## 6 Solution

Appliquer les correctifs (se référer à la section Documentation).

## 7 Documentation

- Avis du CERT/CC :  
<http://www.cert.org/advisories/CA-2002-10.html>
- Bulletin Sun Alert Notification #44502 :  
[http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F44502&zone\\_32=category%3Asecurity](http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F44502&zone_32=category%3Asecurity)

## Gestion détaillée du document

**06 mai 2002** version initiale.

**03 juin 2002** ajout du lien vers avis Sun.