

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-2009-AVI-268>

---

### Gestion du document

Référence	CERTA-2009-AVI-268
Titre	Multiples vulnérabilités dans Sun Solaris
Date de la première version	07 juillet 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Sun #262668 #262048 du 30 juillet 2009
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 à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Sun Solaris 10.

## 3 Résumé

Deux vulnérabilités présentes dans le système d'exploitation Sun Solaris permettent à un utilisateur distant de provoquer un déni de service, de porter atteinte à l'intégrité et à la confidentialité des données.

## 4 Description

Deux vulnérabilités sont présentes dans Sun Solaris :

- la première (CVE-2009-2297) concerne la pile UDP (*udp(7p)*) des systèmes Solaris disposant des

*Solaris Trusted Extensions*. Elle permet à un utilisateur distant malintentionné de provoquer un déni de service ;

- la seconde (CVE-2009-2296) est relative à la mise en œuvre du protocole NFSv4 par Solaris et permet à un utilisateur ne disposant pas de droits suffisants d'accéder en lecture ou en écriture à des partages NFS qui lui sont normalement interdits.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Sun Solaris #262048 du 30 juin 2009 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-262048-1>
- Bulletin de sécurité Sun Solaris #262668 du 30 juin 2009 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-262668-1>
- Référence CVE CVE-2009-2296 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2296>
- Référence CVE CVE-2009-2297 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2297>

## Gestion détaillée du document

07 juillet 2009 version initiale.