

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans ZFS pour Sun Solaris et Sun OpenSolaris

---

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-450>

---

### Gestion du document

Référence	CERTA-2009-AVI-450
Titre	Vulnérabilité dans ZFS pour Sun Solaris et Sun OpenSolaris
Date de la première version	16 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun 265908 du 14 octobre 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Solaris 10 pour plateformes SPARC avec le correctif 137137-09 et sans le correctif 141444-09 ;
- Solaris 10 pour plateformes x86 avec le correctif 137138-09 et sans le correctif 141445-09 ;
- OpenSolaris pour plateformes SPARC et x86, versions snv\_100 à snv\_117.

## 3 Résumé

Une vulnérabilité affectant le système de fichiers ZFS intégré aux systèmes d'exploitation Sun Solaris et Sun OpenSolaris a été corrigée. Elle permet de contourner la politique de sécurité du système et d'atteindre à la confidentialité des données.

## **4 Description**

Une vulnérabilité affectant le système de fichiers ZFS intégré aux systèmes d'exploitation Sun Solaris et Sun OpenSolaris a été corrigée. Elle permet à une personne malintentionnée, possédant un compte utilisateur aux droits restreints, de s'approprier des fichiers appartenant à un autre utilisateur.

## **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 #265908 du 14 octobre 2009 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-265908-1>

## **Gestion détaillée du document**

**16 octobre 2009** version initiale.