

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la commande passwd sur Sun

---

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-2004-AVI-069>

---

### Gestion du document

Référence	CERTA-2004-AVI-069
Titre	Vulnérabilité de la commande passwd sur Sun
Date de la première version	08 mars 2004
Date de la dernière version	–
Source(s)	Buletin de sécurité 57454 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

Elévation de privilèges.

## 2 Systèmes affectés

- Solaris 8 sur architecture Sparc avec les correctifs 108993-14 à 108993-31 ;
- Solaris 8 sur architecture x86 avec les correctifs 108994-14 à 108994-31 ;
- Solaris 9 sur architecture Sparc et x86.

La version Solaris 7 n'est pas affectée par cette vulnérabilité.

## 3 Description

Une vulnérabilité sur la commande `passwd` permet à un utilisateur local mal intentionné d'obtenir les privilèges du super utilisateur (`root`).

## 4 Solution

Appliquer le correctif, correspondant à votre système d'exploitation et votre architecture, disponible sur le site de SUN (cf. section documentation).

## 5 Documentation

- Avis de sécurité 57454 de SUN :  
[http://www.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57454&zone\\_32=category%3Asecurity](http://www.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57454&zone_32=category%3Asecurity)
- Correctif 108993-32 pour Solaris 8 sur architecture Sparc :  
<http://www.sun.com/pub-cgi/findPatch.pl?PatchId=108993&rev=32>
- Correctif 108994-32 pour Solaris 8 sur architecture x86 :  
<http://www.sun.com/pub-cgi/findPatch.pl?PatchId=108994&rev=32>
- Correctif 113476-11 pour Solaris 9 sur architecture Sparc :  
<http://www.sun.com/pub-cgi/findPatch.pl?PatchId=113476&rev=11>
- Correctif 114242-07 pour Solaris 9 sur architecture x86 :  
<http://www.sun.com/pub-cgi/findPatch.pl?PatchId=114242&rev=07>
- Avis de sécurité O-088 du CIAC :  
<http://www.ciac.org/ciac/bulletins/o-088.shtml>

## Gestion détaillée du document

08 mars 2004 version initiale.