



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 31 juillet 2003  
N° CERTA-2003-AVI-127-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans l'éditeur de liens dynamiques sur 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-2003-AVI-127>

---

### Gestion du document

Référence	CERTA-2003-AVI-127-001
Titre	Vulnérabilité dans l'éditeur de liens dynamiques sur Solaris
Date de la première version	31 juillet 2003
Date de la dernière version	1 août 2003
Source(s)	Avis de sécurité de iDefense
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 2.6 ;
- Solaris 7 ;
- Solaris 8 ;
- Solaris 9.

### 3 Résumé

Une vulnérabilité présente sur l'éditeur de liens dynamiques sous Solaris permet à un utilisateur local mal intentionné du système d'obtenir les privilèges du super-utilisateur.

## 4 Description

L'éditeur de liens dynamiques (ld.so.1) permet à des exécutable d'utiliser des bibliothèques dynamiques. La variable LD\_PRELOAD, qui contient les chemins d'accès à ces bibliothèques, permet le chargement des bibliothèques.

Un utilisateur mal intentionné peut, en exécutant un programme « setuid root », provoquer un débordement de pile, par le biais de la variable LD\_PRELOAD et obtenir les droits du super-utilisateur (root).

## 5 Solution

Appliquer le correctif correspondant à votre plate-forme (cf. section documentation).

## 6 Documentation

- Correctifs de Sun :  
<http://sunsolve.sun.com/securitypatch>
- Avis de sécurité Sun :  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/55680>
- Référence CVE CAN-2003-0609 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0609>
- Avis de sécurité de iDefense :  
<http://www.iddefense.com/advisory/07.29.03.txt>

## Gestion détaillée du document

**31 juillet 2003** version initiale.

**1 août 2003** ajout de l'avis Sun et de la référence CVE.