



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 février 2007
N° CERTA-2007-AVI-065

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-2007-AVI-065>

Gestion du document

Référence	CERTA-2007-AVI-065
Titre	Multiples vulnérabilités dans Sun Solaris
Date de la première version	02 février 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun 102724 du 12 décembre 2006
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 ;
- déni de services ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Sun Solaris 8 (x86 et SPARC) ;
- Sun Solaris 9 (x86 et SPARC) ;
- Sun Solaris 10 (x86 et SPARC).

3 Résumé

Deux vulnérabilités présentes dans l'éditeur de liens dynamiques de Sun Solaris permettent, une fois combinées, de contourner la politique de sécurité ou d'exécuter du code arbitraire.

4 Description

L'éditeur de liens dynamiques `ld.so` de Sun Solaris possède deux vulnérabilités.

La première vulnérabilité permet à un utilisateur local de contourner la politique de sécurité après avoir au préalable modifié la valeur de certaines variables d'environnement locales afin d'accéder à des données protégées.

La seconde vulnérabilité permet, par le biais d'un débordement de mémoire, d'exécuter du code arbitraire. Cette vulnérabilité n'est exploitable qu'en utilisant les droits du super utilisateur (`root`).

En parvenant à combiner ces deux vulnérabilités, un utilisateur local non privilégié peut exécuter du code arbitraire en usurpant les droits du super utilisateur (`root`).

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 102724 du 12 décembre 2006 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102724-1>
- Référence CVE CVE-2006-6495 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6495>

Gestion détaillée du document

02 février 2007 version initiale.