Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 décembre 2008
N° CERTA-2008-AVI-600

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSL de Sun Solaris

Gestion du document

Référence	CERTA-2008-AVI-600
Titre	Vulnérabilité dans OpenSSL de Sun Solaris
Date de la première version	11 décembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun #246846
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.

2 Systèmes affectés

- Sun Solaris 10 pour architecture SPARC ;
- Sun Solaris 10 pour architecture x86.

3 Résumé

Une vulnérabilité dans la version de `OpenSSL` pour `Sun Solaris 10` permet à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Une erreur est présente dans le moteur de traitement des fichiers au format `PKCS#11` de `OpenSSL` pour `Sun Solaris 10`. Cette vulnérabilité peut engendrer des corruptions de mémoire cache interne dans `OpenSSL`.

Ainsi, un utilisateur distant malintentionné peut provoquer un déni de service de `OpenSSL` ou d'une application s'appuyant sur ce dernier par le biais d'un fichier au format `PKCS#11` construit de façon particulière.

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 #246846 du 03 décembre 2008 :
http://sunsolve.sun.com/search/document.do?assetkey=1-66-246846-1

Gestion détaillée du document

11 décembre 2008 version initiale.