



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 juillet 2007  
N° CERTA-2007-AVI-302

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Sun Java Secure Socket Extension

---

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-302>

---

### Gestion du document

Référence	CERTA-2007-AVI-302
Titre	Vulnérabilité dans Sun Java Secure Socket Extension
Date de la première version	11 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Sun du 10 juillet 2007
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 Java Secure Socket Extension (JSSE) 1.x;
- Sun Java JDK 1.5.x;
- Sun Java JDK 1.6.x;
- Sun Java JRE 1.4.x;
- Sun Java JRE 1.5.x (5.x);
- Sun Java JRE 1.6.x (6.x);
- Sun Java SDK 1.4.x.

## 3 Résumé

Une vulnérabilité dans Sun Java Secure Socket Extension permet à un utilisateur distant de provoquer un déni de service.

## **4 Description**

Une erreur dans la mise en œuvre de l'initialisation de connexions en SSL/TLS par Sun Java Secure Socket Extension permet à un utilisateur distant de provoquer un déni de service de l'application utilisant cette extension par le biais d'une requête construite 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 #102997 du 10 juillet 2007 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102997-1>

## **Gestion détaillée du document**

**11 juillet 2007** version initiale.