



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 05 décembre 2006  
N° CERTA-2006-AVI-528

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Sun Java System

---

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-2006-AVI-528>

---

### Gestion du document

Référence	CERTA-2006-AVI-528
Titre	Vulnérabilité dans Sun Java System
Date de la première version	05 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun #102733 du 30 novembre 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

- Contournement de la politique de sécurité ;
- pollution du cache du serveur mandataire (proxy) ;
- attaques de type Cross Site Scripting.

## 2 Systèmes affectés

- Sun Java System Application Server (Sun ONE) 7.x ;
- Sun Java System Application Server 8.x ;
- Sun Java System Web Proxy Server 3.x ;
- Sun Java System Web Proxy Server 4.x ;
- Sun Java System Web Server (Sun ONE/iPlanet) 6.x.

## 3 Résumé

Une vulnérabilité dans les produits Sun Java System permet à un utilisateur distant malintentionné de contourner la politique de sécurité, de réaliser des attaques de type Cross Site Scripting ou de polluer le cache du serveur.

## **4 Description**

Une vulnérabilité dans certaines applications Sun Java System est causée par une erreur dans la gestion des requêtes HTTP par Sun Java System Proxy Server, dans la mesure où Sun Java System Web Server ou Sun Java System Application Server est installé sur le système. Cette vulnérabilité peut être exploitée par un utilisateur distant malintentionné afin de réaliser une attaque de type Cross Site Scripting ou de contourner la politique de sécurité ou de compromettre le cache du serveur web mandataire.

## **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 #102733 du 30 novembre 2006 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102733-1>

## **Gestion détaillée du document**

**05 décembre 2006** version initiale.