



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 janvier 2008  
N° CERTA-2008-AVI-024

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Sun Java System Identity Manager

---

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-2008-AVI-024>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2008-AVI-024   |
| Titre                       | Multiples vulnérabilités dans Sun Java System Identity Manager |
| Date de la première version | 16 janvier 2008  |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité Sun #103180 du 14 janvier 2008            |
| 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 ;
- injection de code indirecte.

## 2 Systèmes affectés

- Sun Java System Identity Manager 6.0 ;
- Sun Java System Identity Manager 6.0 SP1 ;
- Sun Java System Identity Manager 6.0 SP2 ;
- Sun Java System Identity Manager 7.0 ;
- Sun Java System Identity Manager 7.1.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans Sun Java Identity Manager et permettent un contournement de la politique de sécurité via une injection de code indirecte.

## 4 Description

De multiples vulnérabilités dans Sun Java Identity Manager permettent à un individu malveillant :

- l'exécution de script en local ou à distance via une vulnérabilité de type injection de code indirecte (*Cross Site Scripting*) dans le navigateur d'un utilisateur cliquant sur un lien vers Sun Java System Identity Manager ;
- l'injection de code *HTML* en local ou à distance dans le navigateur d'un utilisateur cliquant sur un lien vers Sun Java System Identity Manager ;
- la redirection vers un site externe ou l'injection d'un cadre (*frame*) contenant des données.

## 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 #103180 du 14 janvier 2008 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103180-1>

## Gestion détaillée du document

**16 janvier 2008** version initiale.