



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 17 janvier 2007  
N° CERTA-2007-AVI-033-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la machine virtuelle Java de Sun

---

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-033>

---

### Gestion du document

Référence	CERTA-2007-AVI-033-001
Titre	Vulnérabilité dans la machine virtuelle Java de Sun
Date de la première version	17 janvier 2007
Date de la dernière version	17 février 2007
Source(s)	Bulletin de sécurité Sun #102760 du 16 janvier 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Sun Java JDK 1.5.x ;
- Sun Java JDK 1.4.x ;
- Sun Java JDK 1.3.x ;
- Sun Java JRE 1.5.x ;
- Sun Java JRE 1.4.x ;
- Sun Java JRE 1.3.x.

## 3 Résumé

Une vulnérabilité dans la machine virtuelle Java de Sun permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

## 4 Description

Une erreur dans la mise en œuvre de la lecture des images au format GIF permet d'effectuer une attaque de type débordement de mémoire sur la machine virtuelle Java de Sun. Cette vulnérabilité permet à un utilisateur distant d'exécuter du code arbitraire par le biais d'une image au format GIF 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 Solaris #102760 du 16 janvier 2007 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102760-1>
- Bulletin Gentoo GLSA 200702-07 / java du 17 février 2007 :  
<http://www.gentoo.org/security/en/glsa/glsa-200702-07.xml>
- Référence CVE CVE-2007-0243 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0243>

## Gestion détaillée du document

**17 janvier 2007** version initiale.

**19 février 2007** ajout de la référence Gentoo.