



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 1 avril 2003  
N° CERTA-2002-AVI-056-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la machine virtuelle Java

---

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-2002-AVI-056>

---

### Gestion du document

Référence	CERTA-2002-AVI-056-002
Titre	Vulnérabilité de la machine virtuelle Java
Date de la première version	19 mars 2002
Date de la dernière version	01 avril 2003
Source(s)	Seconde version du bulletin de sécurité Microsoft MS02-013 Bulletin de sécurité #00218 de Sun Bulletin de sécurité SSRT0822 de Compaq
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

Elévation de privilèges.

## 2 Systèmes affectés

Plusieurs implémentations de machines virtuelles Java livrées sur de nombreux systèmes d'exploitation (Solaris, Linux, Windows, HP-UX, Tru64 Unix, OpenVms, Irix), des navigateurs (Internet Explorer, Netscape Navigator) ou outils de supervision (Compaq Insight Manager, Compaq Management Agent).

Pour connaître les versions des systèmes affectés par cette vulnérabilité, consultez les différents bulletins de sécurité mentionnés à la section Documentation.

## 3 Résumé

Il est possible d'exécuter du code arbitraire avec les privilèges de l'utilisateur grâce à une applique Java habilement conçue.

## 4 Description

Une vulnérabilité d'un composant de la machine virtuelle Java (*JRE Bytecode Verifier* chez Sun et *Virtual Machine Verifier* chez Microsoft), permet à un utilisateur mal intentionné d'exécuter du code arbitraire en contournant les mécanismes de sécurité restreignant les privilèges d'une applique (*Sandbox*) s'exécutant dans une machine virtuelle Java.

## 5 Solution

Appliquez le correctif fourni par l'éditeur :

- Bulletin de sécurité #00218 de Sun :  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?type=0&doc=secbull%2F218&display=plain>
- Bulletin de sécurité MS02-013 de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/MS02-013.asp>
- Bulletin de sécurité HPSBUX0203-186 de Hewlett-Packard :  
<http://archives.neohapsis.com/archives/hp/2002-q1/0084.html>
- Bulletin de sécurité SSRT0822 de Compaq :  
<http://archives.neohapsis.com/archives/tru64/2002-q2/0021.html>
- Avis de sécurité Netscape :  
<http://www.netscape.com/security/>
- Bulletin de sécurité 20030303-01-I de SGI :  
<ftp://patches.sgi.com/support/free/security/advisories/20030303-01-I>

## 6 Documentation

Référence CVE CAN-2002-0076 :

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0076>

### Gestion détaillée du document

**19 mars 2002** version initiale.

**06 juin 2002** seconde version : prise en compte du bulletin de sécurité SSRT0822 de Compaq.

**01 avril 2003** ajout bulletin de sécurité de SGI. Ajout référence CVE.