

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la machine virtuelle Java (JRE) 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-2004-AVI-377>

---

### Gestion du document

Référence	CERTA-2004-AVI-377-005
Titre	Vulnérabilité dans la machine virtuelle Java de SUN
Date de la première version	23 novembre 2004
Date de la dernière version	24 février 2005
Source(s)	Bulletin de sécurité iDefense du 22 novembre 2004
Pièce(s) jointe(s)	

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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Ces vulnérabilités affectent :

- JRE 1.3.x et versions antérieures ;
- JRE 1.4.x et versions antérieures ;
- SDK 1.3.x et versions antérieures ;
- SDK 1.4.x et versions antérieures.

sur les plates-formes Windows, Solaris et Linux. JDK et JRE 5.0 ne sont pas affectés par cette vulnérabilité.

## 3 Résumé

Une vulnérabilité présente dans la machine virtuelle Java permet à une personne mal intentionnée de contourner les mesures de sécurité imposées par un applet.

## 4 Description

Le JRE (Java Runtime Environment) permet l'exécution de code java.

Cette vulnérabilité, présente dans le JRE, est due à une mauvaise gestion lors de l'échange de données entre le code Java et JavaScript. Au moyen d'un site web malicieusement constitué, une personne malveillante peut porter atteinte à l'intégrité et à la confidentialité des données présentes sur le système. elle peut également exécuter du code arbitraire à distance avec les privilèges de la victime.

## 5 Contournement provisoire

Désactiver dans le navigateur internet la machine virtuelle Java et JavaScript, cela a pour effet de rendre inexploitable cette vulnérabilité.

## 6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

## 7 Documentation

- Site de l'éditeur :  
<http://java.sun.com>
- Bulletin de sécurité Sun #57591 du 22 novembre 2004 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1>
- Bulletin de sécurité iDEFENSE du 22 novembre 2004 :  
<http://www.odefense.com/application/poi/display?id=158>
- Mise à jour de sécurité des paquetages NetBSD sun-jre14, sun-jdk14, sun-jre13 et sun-jdk13 :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/lang/sun-jre14/README.html>  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/lang/sun-jdk14/README.html>  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/lang/sun-jre13/README.html>  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/lang/sun-jdk13/README.html>
- Bulletin de sécurité FreeBSD pour jdk du 25 novembre 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité Gentoo GLSA 200411-38 du 29 novembre 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200411-38.xml>
- Bulletin de sécurité HP HPSBUX01100 du 01 décembre 2004 :  
<http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01100>
- Bulletin de sécurité Apple MacOS X 2005-002 du 22 février 2005 :  
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CAN-2004-1029 :  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1029>

## Gestion détaillée du document

**23 novembre 2004** version initiale.

**24 novembre 2004** ajout des références aux mises à jour de sécurité NetBSD.

**26 novembre 2004** ajout de la référence au bulletin de sécurité FreeBSD.

**30 novembre 2004** ajout de la référence au bulletin de sécurité Gentoo.

**01 décembre 2004** ajout de la référence au bulletin de sécurité HP HPSBUX01100.

**24 février 2005** ajout de la référence au bulletin de sécurité Apple MacOS X.