

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Oracle 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-2010-AVI-152>

---

### Gestion du document

Référence	CERTA-2010-AVI-152
Titre	Multiples vulnérabilités dans Oracle Java
Date de la première version	01 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle Java de mars 2010
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Java SE, JDK/JRE 6 Update 18 et antérieures pour Windows, Solaris, et Linux ;
- Java SE, JDK 5.0 Update 23 et antérieures pour Solaris ;
- Java SE, SDK 1.4.2\_25 et antérieures pour Solaris ;
- Java for Business, JDK/JRE 6 Update 18 et antérieures pour Windows, Solaris, et Linux ;
- Java for Business, JDK/JRE 5.0 Update 23 et antérieures pour Windows, Solaris, et Linux ;
- Java for Business, SDK/JRE 1.4.2\_25 et antérieures pour Windows, Solaris, et Linux.

## 3 Résumé

Plusieurs vulnérabilités découvertes dans Oracle Java peuvent être exploitées par un utilisateur malintentionné afin de compromettre le système ou d'entraver son bon fonctionnement.

## 4 Description

De multiples vulnérabilités ont été découvertes dans Oracle Java :

- une erreur dans le code de la classe `HeadspaceSoundbank` peut provoquer un débordement de mémoire par le biais d'un fichier `Soundbank` spécialement conçu ;
- une erreur dans le traitement des images peut provoquer un débordement de mémoire par le biais d'une applet Java spécialement conçue ;
- plusieurs autres vulnérabilités non précisées sont présentes dans les composants Oracle Java.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Oracle Java de mars 2010 :  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/javacpumar2010.html>
- Référence CVE CVE-2009-3335 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3335>
- Référence CVE CVE-2010-0082 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0082>
- Référence CVE CVE-2010-0084 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0084>
- Référence CVE CVE-2010-0085 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0085>
- Référence CVE CVE-2010-0087 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0087>
- Référence CVE CVE-2010-0088 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0088>
- Référence CVE CVE-2010-0089 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0089>
- Référence CVE CVE-2010-0090 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0090>
- Référence CVE CVE-2010-0091 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0091>
- Référence CVE CVE-2010-0092 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0092>
- Référence CVE CVE-2010-0093 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0093>
- Référence CVE CVE-2010-0094 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0094>
- Référence CVE CVE-2010-0095 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0095>
- Référence CVE CVE-2010-0837 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0837>
- Référence CVE CVE-2010-0838 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0838>
- Référence CVE CVE-2010-0839 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0839>
- Référence CVE CVE-2010-0840 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0840>
- Référence CVE CVE-2010-0841 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0841>

- Référence CVE CVE-2010-0842 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0842>
- Référence CVE CVE-2010-0843 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0843>
- Référence CVE CVE-2010-0844 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0844>
- Référence CVE CVE-2010-0845 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0845>
- Référence CVE CVE-2010-0846 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0846>
- Référence CVE CVE-2010-0847 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0847>
- Référence CVE CVE-2010-0848 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0848>
- Référence CVE CVE-2010-0849 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0849>
- Référence CVE CVE-2010-0850 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0850>

## **Gestion détaillée du document**

**01 avril 2010** version initiale.