

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Sun Java Runtime Environment (JRE)

---

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-366>

---

### Gestion du document

Référence	CERTA-2007-AVI-366
Titre	Vulnérabilité de Sun Java Runtime Environment (JRE)
Date de la première version	16 août 2007
Date de la dernière version	–
Source(s)	Document Sun 103024 du 15 août 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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- JDK et JRE 5.0 ayant une mise à jour antérieure à Update 10 ;
- SDK et JRE antérieurs à 1.4.2\_15 ;
- J2SE 5.0 ayant une mise à jour antérieure à Update 12 ;
- J2SE antérieur à la version actuelle 1.4.2.

## 3 Résumé

Une vulnérabilité a été identifiée dans l'environnement Java JRE (*Java Runtime Environment*). L'exploitation de cette dernière permettrait à une personne malveillante, par le biais d'une applet, d'exécuter du code arbitraire sur la machine vulnérable, avec les droits de l'utilisateur.

## 4 Description

Une vulnérabilité a été identifiée dans l'environnement Java JRE (*Java Runtime Environment*). Par exemple, une personne malveillante pourrait, par le biais d'une applet spécialement construite, exécuter du code arbitraire sur la machine de l'utilisateur chargeant ce code. L'applet élèverait ses privilèges à ceux de l'utilisateur connecté, pouvant ainsi écrire et lire des fichiers.

## 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 #103024 du 15 août 2007 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103024-1>
- Site Sun Java distribuant les mises à jour :  
<http://java.sun.com/>

## Gestion détaillée du document

16 août 2007 version initiale.