



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 03 septembre 2009  
N° CERTA-2009-AVI-365

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans IBM 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-2009-AVI-365>

---

### Gestion du document

Référence	CERTA-2009-AVI-365
Titre	Vulnérabilités dans IBM Java
Date de la première version	03 septembre 2009
Date de la dernière version	–
Source(s)	
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 ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- IBM Java 5.x :
- IBM Java 6.x.

## 3 Résumé

Plusieurs vulnérabilités dans IBM Java permettent à un utilisateur distant malintentionné de porter atteinte à la confidentialité et à l'intégrité des données, de contourner la politique de sécurité, de provoquer un déni de service ou encore d'exécuter du code arbitraire avec des privilèges élevés.

## 4 Description

- Une vulnérabilité dans le système audio du Java Runtime Environment peut être exploitée afin de porter atteinte à la confidentialité des propriétés du système (CVE-2009-2670) ;
- trois vulnérabilités dans la mise en œuvre du serveur mandataire (*proxy*) dans Java Runtime Environment permettent à un utilisateur de porter atteinte à la confidentialité des données et d’obtenir un *cookie* de session de navigation ou de réaliser des connexions non autorisées depuis le système vulnérable (CVE-2009-2671, CVE-2009-2672 et CVE-2009-2673) ;
- une vulnérabilité de type débordement de mémoire permet à un utilisateur de faire exécuter une applique Java non-sûre avec des privilèges élevés (CVE-2009-2675).
- une vulnérabilité présente dans l’appliquette `JNLPAppletLauncher` permet à un utilisateur distant malveillant de porter atteinte à l’intégrité du système et potentiellement d’exécuter du code arbitraire sous la forme d’une applique.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité IBM Java du 10 août 2009 :  
<http://www.ibm.com/developerworks/java/jdk/alerts/>
- Bulletin de sécurité RedHat RHSA-2009:1199 du 06 août 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1199.html>
- Bulletin de sécurité RedHat RHSA-2009:1200 du 06 août 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1200.html>
- Bulletin de sécurité RedHat RHSA-2009:1201 du 06 août 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1201.html>
- Bulletin de sécurité RedHat RHSA-2009:1236 du 28 août 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1236.html>
- Bulletin de sécurité Ubuntu USN-814-1 du 11 août 2009 :  
<http://www.ubuntu.com/usn/usn-814-1>
- Bulletin de sécurité SuSE SUSE-SA:2009:043 du 07 août 2009 :  
[http://www.novell.com/linux/security/advisories/2009\\_43\\_sunjava.html](http://www.novell.com/linux/security/advisories/2009_43_sunjava.html)
- Référence CVE CVE-2009-2670 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2670>
- Référence CVE CVE-2009-2671 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2671>
- Référence CVE CVE-2009-2672 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2672>
- Référence CVE CVE-2009-2673 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2673>
- Référence CVE CVE-2009-2675 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2675>
- Référence CVE CVE-2009-2676 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2676>

## Gestion détaillée du document

03 septembre 2009 version initiale.