



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 août 2007
N° CERTA-2007-AVI-349

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la machine virtuelle Java 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-2007-AVI-349>

Gestion du document

Référence	CERTA-2007-AVI-349
Titre	Vulnérabilité dans la machine virtuelle Java de Sun
Date de la première version	07 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Sun 102995 du 18 juillet 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- JDK et JRE 6 Update 1;
- JDK et JRE 5.0 Update 11;
- SDK et JRE 1.4.2_12.

Ainsi que les versions antérieures de ces différentes distributions.

3 Résumé

Une vulnérabilité dans le chargeur d'*applet* du Java Runtime Environment permet de contourner la politique de sécurité liée à l'exécution d'une *applet*.

4 Description

Une vulnérabilité dans le chargeur d'*applet* du Java Runtime Environment permet à une *applet* chargée depuis un site distant et qui s'exécute localement d'accéder aux services présents sur la machine sans respecter la politique de sécurité du réseau. Cela permettrait par exemple d'exploiter les vulnérabilités potentielles des services présents sur la machine alors qu'ils ne sont normalement pas accessibles.

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 Solaris #102995 du 18 juillet 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102995-1>
- Bulletin de sécurité RedHat RHSA-2007:0818 du 06 août 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0818.html>
- Référence CVE CVE-2007-3922 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3922>

Gestion détaillée du document

07 août 2007 version initiale.