



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 octobre 2004
N° CERTA-2004-AVI-264-001

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-264>

Gestion du document

Référence	CERTA-2004-AVI-264-001
Titre	Vulnérabilité dans la machine virtuelle Java (JRE) de SUN
Date de la première version	05 août 2004
Date de la dernière version	22 octobre 2004
Source(s)	Bulletin de sécurité #57613 de SUN
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

- Elévation de privilèges ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Ces vulnérabilités affectent :

- SDK et JRE versions 1.4.2_04 et antérieures ;
- SDK et JRE versions 1.4.1_07 et antérieures ;
- SDK et JRE versions 1.4.0_04 et antérieures.

sur les plates-formes Windows, Solaris et Linux. Les versions antérieures à 1.4.0 de SDK et JRE ne sont pas affectées par ces vulnérabilités.

3 Résumé

Une vulnérabilité présente dans le processeur XSLT (Extensible Stylesheet Language Transformation) de la machine virtuelle java (JRE) permet à une applet non privilégiée de lire les données d'une autre applet traitée par le processeur XSLT et d'élever ses privilèges.

4 Description

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

XSLT (Extensible Stylesheet Language Transformation) est un processeur inclu dans le JRE, destiné à réécrire des documents XML (eXtensible Markup Language) vers un format différent.

Une vulnérabilité présente dans le JRE permet à un utilisateur mal intentionné de récupérer des données d'une applet, et d'élever ses privilèges au moyen d'une applet malicieuse contenue dans une page HTML.

5 Solution

Mettre à jour SDK et JRE avec la version 1.4.2_05 ou supérieure :

<http://java.sun.com/j2se/>

6 Documentation

- Bulletin de sécurité #57613 de SUN du 2 août 2004 :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57613>
- Bulletin de sécurité HPSBUX01087 du 12 octobre 2004 :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01087>

Gestion détaillée du document

05 août 2004 version initiale.

22 octobre 2004 ajout référence au bulletin de sécurité HPSBUX01087 de HP.