Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 janvier 2003
N° CERTA-2003-AVI-016

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du plug-in Java, Java Web Start et JSSE

Gestion du document

Référence	CERTA-2003-AVI-016
Titre	Vulnérabilité de JSSE, du plug-in Java et de Java Web Start
Date de la première version	28 janvier 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Sun 50081
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 ;
- déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- JSSE faisant partie de Java SDK et JRE version 1.4.0_01 et versions antérieures de la série 1.4.0 ;
- JSSE version 1.0.3 et versions antérieures ;
- plug-in Java faisant partie de Java SDK et JRE version 1.4.1 ;
- plug-in Java faisant partie de Java SDK et JRE version 1.4.0_02 et versions antérieures de la série 1.4.0 ;
- plug-in Java faisant partie de Java SDK et JRE version 1.3.1_05 et versions antérieures de la série 1.3.1 ;
- plug-in Java faisant partie de Java SDK et JRE version 1.3.0_05 et versions antérieures de la série 1.3.0 ;
- Java Web Start version 1.2 ;
- Java Web Start version 1.0.1_02 et versions antérieures de la série 1.0.1 ;
- Java Web Start version 1.0 ;

3 Résumé

Une vulnérabilité dans la validation des certificats par JSSE (Java Secure Socket Extension), le plug-in Java et Java Web Start permet à un utilisateur mal intentionné d'exécuter du code malicieux à distance.

4 Description

JSSE (Java Secure Socket Extension) est une extension du langage Java implémentant une version Java des protocoles SSL (Socket Secure Layer) et TLS (Transport Socket Layer) ainsi que des fonctionnalités de chiffrement, de contrôle d'intégrité et d'authentification.

Java Web Start permet de lancer des applications Java directement depuis un navigateur. Si l'application n'est pas présente en locale sur la machine, Java Web Start s'occupe du téléchargement des fichiers nécessaires (archives JAR signées).

Une vulnérabilité dans la vérification des certificats par JSSE (Java Secure Socket Extension), par le plug-in Java et par Java Web Start permet à un utilisateur mal intentionné d'exécuter du code malicieux à distance.

5 Solution

Effectuer les mises à jour de Java SDK et Java JRE comme indiqué dans le bulletin de sécurité de Sun (Cf. section Documentation).

6 Documentation

Bulletin de sécurité 50081 de Sun :
http://sunsolve.sun.com/pub-cgi/secBulletin.pl

Gestion détaillée du document

28 janvier 2003 version initiale.
01 avril 2003 les modifications au présent avis figurent dans l'avis CERTA-2003-AVI-020.