

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous JSSE, Java Plug-In et Java Web Start

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-2003-AVI-020>

Gestion du document

Référence	CERTA-2003-AVI-020-001
Titre	Vulnérabilité sous JSSE, Java Plug-In et Java Web Start
Date de la première version	07 février 2003
Date de la dernière version	01 avril 2003
Source(s)	Avis de sécurité #50081 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

Contournement de la politique de sécurité.

2 Systèmes affectés

JSSE (Java Secure Socket Extension) est une extension du langage Java implémentant une version Java des protocoles SSL (Socket Secure Layer) et TLS (Transport Layer Security) 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).

Java Plug-In est une extension permettant à un navigateur d'utiliser la machine virtuelle Java de Sun livrée avec le Software Development Kit (SDK) ou le Java Runtime Environment (JRE).

Se référer aux bulletins de sécurité des différents éditeurs (cf. section Documentation) pour obtenir la liste des versions affectées.

3 Description

Sun a publié un bulletin de sécurité (cf. section Documentation) indiquant qu'une vulnérabilité existe dans le contrôle des certificats électroniques :

- lors de connexions via SSL, une erreur dans la validation du certificat peut entraîner l'authentification de sites non sûrs ;
- lors de la vérification de la signature d'un code (archive JAR), une erreur dans la validation du certificat peut entraîner l'exécution d'un code non sûr.

4 Solution

Se référer aux bulletins de sécurité des différents éditeurs (cf. section Documentation) pour l'obtention des correctifs.

5 Documentation

- Bulletin de sécurité #50081 de Sun :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50081>
- Bulletin de sécurité HPSBUX0301-239 de Hewlett-Packard :
<http://itrc.hp.com>
- Bulletin de sécurité 20030303-01-I de SGI :
<ftp://patches.sgi.com/support/free/security/advisories/20030303-01-I>

Gestion détaillée du document

07 février 2003 version initiale.

01 avril 2003 ajout bulletin de sécurité de SGI