Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 mai 2004
N° CERTA-2004-AVI-169

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Java Secure Socket Extension (JSSE)

Gestion du document

Référence	CERTA-2004-AVI-169
Titre	Vulnérabilité de Java Secure Socket Extension (JSSE)
Date de la première version	19 mai 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité #57560 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

Usurpation d'identité.

2 Systèmes affectés

JSSE 1.0.3, 1.0.3_01 et 1.0.3_02 pour les plates-formes Linux, Solaris et Windows.
La version de JSSE intégrée à JAVA 2 SDK 1.4.x n'est pas vulnérable.

3 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. JSSE à été intégré à JAVA 2 SDK version 1.4.

Selon Sun, une vulnérabilité est présente dans la validation des certificats permettant ainsi à un site web malicieux de se faire passer pour un site de confiance lors d'une connexion SSL.

4 Solution

La version 1.0.3_03 de JSSE corrige cette vulnérabilité :
http://java.sun.com/products/jsse/index-103.html

5 Documentation

Bulletin de sécurité #57560 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57560

Gestion détaillée du document

19 mai 2004 version initiale.