Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 juin 2002
N° CERTA-2002-AVI-050-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la machine virtuelle Java

Gestion du document

Référence	CERTA-2002-AVI-050-001
Titre	Vulnérabilité de la machine virtuelle Java
Date de la première version	05 mars 2002
Date de la dernière version	06 juin 2002
Source(s)	bulletin de sécurité 00216 de Sun Avis de sécurité Netscape Bulletin de sécurité Microsoft MS02-013 Bulletin de sécurité SSRT0822 de Compaq
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 ;
- divulgation de données ;
- déni de service ;
- attaque de type *man in the middle* (attaque par le milieu).

2 Systèmes affectés

Tous les systèmes utilisant une machine virtuelle Java basée sur celle de Sun.
Entre autres :

- Les machines virtuelles de SDK et JRE versions 1.3.0_02 et antérieures sous Solaris et Linux ;
- les machines virtuelles de SDK et JRE versions 1.2.2_010 et antérieures sous Solaris et Linux ;
- les machines virtuelles de JDK et JRE versions 1.1.8_007 et antérieures sous Solaris et Linux ;
- les navigateurs de Netscape versions 4.79 et antérieurs ainsi que 6, 6.01 et 6.1 ;

- les navigateurs Internet Explorer 4.x, 5.x ;
- les systèmes d'exploitations Micorosoft Windows 98, ME et 2000 pour lesquels la machine virtuelle Java (JVM) est installée par défaut.
- Différents systèmes d'exploitation et logiciels distribués par Compaq.

3 Résumé

Un utilisateur mal intentionné peut, au moyen d'une vulnérabilité de la machine virtuelle Java du navigateur de sa victime, détourner et modifier le flux de données situé entre celle-ci et son serveur mandataire (*Proxy*).

4 Description

Il existe une vulnérabilité de la machine virtuelle de Sun permettant à un utilisateur mal intentionné, par le biais d'une appliquette Java habilement construite, de détourner le flux d'informations circulant entre un client et son serveur mandataire.

Cette vulnérabilité est présente dans la JDK (*Java Developper Kit*) et JRE (*Java Runtime Enviroenment*) de Sun, mais le modèle de la machine virtuelle Java étant le même pour les navigateurs Microsoft et Netscape, elle permet à un utilisateur mal intentionné d'obtenir les données personnelles envoyées sur l'Internet par un utilisateur utilisant ces clients à travers un serveur mandataire, de les utiliser, de les modifier avant leur utilisation, ou bien de les arrêter afin de créer un déni de service.

5 Contournement provisoire

Désactiver Java en attendant d'appliquer le correctif ou la mise à jour du système affecté.

6 Solution

Appliquer le correctif du constructeur :

- Sun : mettre à jour ou changer de version selon les indications du bulletin de sécurité 00216 (cf. : paragraphe Documentation) :
  http://java.sun.com/
- Netscape : passer à la version 6.2 ou 6.2.1 :
  http://www.netscape.com
- Microsoft : mettre à jour la machine virtuelle Java du système :
  http://www.microsoft.com/java/vm/dl_vm40.htm
- Pour connaître les systèmes Compaq affectés ainsi que les mesures à prendre, consulter le bulletin de sécurité SSRT0822 de Compaq (Cf. : paragraphe Documentation).

7 Documentation

- Bulletin de sécurité 00216 de Sun :
  http://sunsolve.sun.com/cgi-bin/secBulletin.pl
- Avis de sécurité Netscape concernant la machine virtuelle Java de Sun:
  http://www.netscape.com/security/
- Bulletin de sécurité MS02-013 de Microsoft :
  http://www.microsoft/com/technet/security/bulletin/MS02-013.asp
- Bulletin de sécurité SSRT0822 de Compaq :
  http://www2.tru64.org/stories.php?story=02/05/14/472385

Gestion détaillée du document

05 mars 2002 version initiale.
06 juin 2002 seconde version : prise en compte du bulletin de sécurité SSRT0822 de Compaq.