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 août 2000
N° CERTA-2000-AVI-032

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la machine virtuelle Java de Microsoft

Gestion du document

Référence	CERTA-2000-AVI-032
Titre	Vulnérabilité dans la machine virtuelle Java de Microsoft
Date de la première version	22 août 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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 lors de la navigation ;
- Accès en lecture à des données non autorisées.

2 Systèmes affectés

Versions des Machines Virtuelles Java concernées :

- Série 2000 ;
- Série 3100 ;
- Série 3200 ;
- Série 3300 ;

sous Windows 9x, NT et 2000.

Nota : Pour connaître la version de la Machine Virtuelle Java utilisée, exécuter la commande `jview` dans une session DOS.

3 Résumé

Un concepteur mal intentionné d'un site internet peut, par le biais d'une application Java, prendre l'identité d'un visiteur de son site pour établir une connexion avec d'autres sites.

4 Description

Par conception une application Java doit seulement pouvoir communiquer avec le site internet visité qui l'accueille. Cependant une vulnérabilité permet à un concepteur mal intentionné d'établir une nouvelle session sous le couvert de l'utilisateur visitant. Ainsi la vulnérabilité peut être employée pour accèder à un site intranet, protégé par un garde barrière, par exemple ou pour accèder à des informations sous l'identité de l'utilisateur.

Bien que cette application puisse se servir des droits d'accès pour s'authentifier sur un site, elle ne permet pas de les compromettre.

5 Solution

Correctif pour la série 2000 (version US) :
http://www.microsoft.com/java/vm/dl_vmsp2.htm

Correctif pour la série 3100 (Version US) :
http://www.microsoft.com/java/vm/dl_vm40.htm
Puis le correctif 3314 (Version US) :
http://download.microsoft.com/download/vm/patch/3314/WIN98Me/EN-US/vmsecfix.exe

Correctif pour les séries 3229-3234 (Version US) :
http://www.microsoft.com/java/vm/dl_vm40.htm
Puis le correctif 3314 (Version US) :
http://download.microsoft.com/download/vm/patch/3314/WIN98Me/EN-US/vmsecfix.exe

Correctif pour la série 3214 (Version US) :
http://download.microsoft.com/download/vm/patch/3314/WIN98Me/EN-US/vmsecfix.exe

Correctif pour les séries 3300 (Version US) :
http://download.microsoft.com/download/vm/patch/3314/WIN98Me/EN-US/vmsecfix.exe

6 Documentation

Bulletin de sécurité de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS00-059.asp

Faq Microsoft :
http://www.microsoft.com/technet/security/bulletin/fq00-059.asp

Gestion détaillée du document

22 août 2000 version initiale.