Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 octobre 2000
N° CERTA-2000-AVI-065

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la Machine Virtuelle Java de Microsoft

Gestion du document

Référence	CERTA-2000-AVI-065
Titre	Vulnérabilité dans la Machine Virtuelle Java de Microsoft
Date de la première version	27 octobre 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

Accès à des données non autorisées.

2 Systèmes affectés

- Microsoft Windows 9x;
- Windows Millenium Edition (ME);
- Windows NT;
- Windows 2000.

3 Résumé

Une vulnérabilité de la machine virtuelle Java de Microsoft Internet Explorer sous Windows permet à l'administrateur d'un site web malicieux de lire des fichiers auxquels il ne devrait pas avoir accès sur le disque dur et dans l'intranet de sa victime.

4 Description

Une vulnérabilité dans la Machine Virtuelle Java de Microsoft Internet Explorer 4.x et 5.x permet à un utilisateur mal intentionné, à l'aide d'un site web habilement conçu, contenant une appliquette java particulière, d'avoir accès en lecture uniquement à tous les fichiers présents sur le disque dur de la machine cliente. Il peut aussi accéder à toutes les données partagées qui sont autorisées pour sa victime dans un intranet, en devinant le chemin d'accès qui est de la forme : `\\machine\chemin\fichier`.

5 Contournement provisoire

Désactiver les java, javascripts, comme indiqué dans les bulletins CERTA-2000-AVI-002, CERTA-2000-ALE-001 et CERTA-2000-ALE-002, CERTA-2000-INF-002.

Couper les connections entre l'intranet et les machines ayant accès à internet.

6 Solution

Une vulnérabilité précédente permettait d'accéder en lecture aux fichiers présents sur le système, en devinant leur chemin d'accès. Peut-être aviez-vous déjà appliquer le correctif correspondant au bulletin de sécurité Microsoft MS00-011 : (

http://www.microsoft.com/technet/security/bulletin/ms00-011.asp)

Mais celui-ci ne corrige pas la vulnérabilité décrite dans le document. Il faut donc appliquer le nouveau correctif de Microsoft. Il dépend du numéro de construction de la Machine Virtuelle installée sur le système.

Cette vulnérabilité est présente dans les Machines Virtuelles Java ayant les numéros de construction suivant :

- 2000 à 2447
- 2752 à 3194
- 3229 à 3240
- 3300 à 3318

Pour connaître le numéro de construction de la Machine Virtuelle qui est installée sur le système, taper la commande `JVIEW` à l'invite de commande.

Installer la nouvelle version de la Machine Virtuelle, dont le numéro de construction est 3319 à l'adresse suivante :

http://www.microsoft.com/java/vm/dl_vm40.htm

7 Documentation

Le bulletin de sécurité Microsoft et sa FAQ et l'article Q277014 de la base de connaissances :

- http://www.microsoft.com/technet/security/bulletin/ms00-081.asp
- http://www.microsoft.com/technet/security/bulletin/fq00-081.asp
- http://support.microsoft.com/support/kb/articles/q277/0/14.asp

Gestion détaillée du document

27 octobre 2000 version initiale.