Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2000
N° CERTA-2000-AVI-059

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la machine virtuelle Java de Microsoft

Gestion du document

Référence	CERTA-2000-AVI-059
Titre	Vulnérabilité dans la machine virtuelle Java de Microsoft
Date de la première version	13 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité de 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

- Exécution de code arbitraire,
- compromission de la machine.

2 Systèmes affectés

Microsoft Windows 9x, Millenium Edition, NT et 2000 ayant installé la machine virtuelle Java de Microsoft (quasiment tous).

3 Résumé

Une vulnérabilité dans la machine virtuelle Java de tous les systèmes Microsoft Windows permet à un utilisateur mal intentionné de faire exécuter par une machine tout ce qui est permis à l'utilisateur courant par le biais d'une appliquette java sur un site web malicieux ou un email au format HTML, par exemple.

4 Description

La machine virtuelle Java de Microsoft contient une fonctionnalité qui permet à une appliquette java de créer, modifier et exécuter un contrôle activeX. Normalement, ceci n'est possible que dans le cas où cette appliquette est exécuté de façon isolée (localement, sur la machine) ou si elle est signée.

Une vulnérabilité dans la machine virtuelle permet à une appliquette java, contenue, par exemple, dans une page web ou un mél au format HTML, de manipuler les contrôles ActiveX, même non marqués « reconnu sûr pour l'écriture de scripts ». Ceci permet à un utilisateur mal intentionné, par le biais d'un site malicieux, ou d'un mél de prendre entièrement possession à distance d'une machine.

5 Solution

Comme indiqué dans les bulletin CERTA-2000-AVI-002, CERTA-2000-ALE-001 et CERTA-2000-ALE-002, CERTA-2000-INF-002 :

Désactiver l'exécution des appliquettes Java et des javascript dans les paramètres de sécurité d'internet explorer et d'Outlook (ou Outlook Express).

Désactiver les contrôles ActiveX dans les paramètres de sécurité d'internet explorer et dans toute application en pemettant l'exécution.

Pour savoir si la machine virtuelle est installée et connaître sa version, taper la commande `JVIEW` à l'invite de commande.

Un numéro de version du type *X.YY.zzzz* apparaît, où zzzz est le numéro de construction. Seules les versions ayant le numéro de construction (*build number*) dans la série 2000, 3100, 3200 et 3300 sont vulnérables.

Appliquer le correctif de Microsoft, dont le numéro de construction sera 3318, pour les séries 3100 à 3300 :
http://www.microsfot.com/java/vm/dl_vm40.htm

Pour la série 2000, il n'existe pas de correctif actuellement.

6 Documentation

- Le bulletin de sécurité Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms00-075.asp
- la FAQ du bulletin :
  http://www.microsoft.com/technet/security/bulletin/fq00-075.asp
- la base de connaissances Microsoft :
  http://www.microsoft.com/technet/support/kb.asp?ID=275609

Gestion détaillée du document

13 octobre 2000 version initiale.