

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Désactivation de l'exécution des fichiers VBS sous Windows

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006>

Gestion du document

Référence	CERTA-2000-INF-006
Titre	Désactivation de l'exécution des fichiers VBS sous Windows
Date de la première version	19 octobre 2000
Date de la dernière version	–
Source(s)	Réseau de confiance
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Systèmes concernés

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

2 Introduction

Les fichiers VBS (Visual Basic Script) sont actuellement très utilisés dans la diffusion, propagation des virus et vers sur Internet. Les installations par défaut de Windows et de ses composants permettent l'exécution automatique de ce type de fichiers par un cliqué double. Une méthode simple pour supprimer ce genre de vulnérabilité des systèmes Windows a été développée.

3 Description

Afin de changer l'application associée à l'ouverture des fichiers possédant une extension particulière, il faut modifier la branche correspondante de la base des registres. Une telle manipulation peut être faite avec n'importe

quel type de fichier, notamment les fichiers à extension en .WSH, .JS, etc.

Ces modifications peuvent être effectuées à la main dans la base des registres avec l'outil `regedit` ou `regedt32`. Cette méthode peut s'avérer dangereuse pour le système et n'est conseillée qu'aux administrateurs qui savent exactement ce qu'ils font.

Plus simplement, il est aussi possible de faire cette association en utilisant les options du menu affichage de l'*explorateur Windows* ou le *poste de travail*. Dans la fenêtre qui apparaît, choisir l'onglet *Types de fichiers*, il est possible de modifier les associations d'applications à tous les formats de fichiers connus par Windows.

Mais dans un soucis de simplification, il existe des possibilités d'automatiser ce genre de tâches avec un fichier qui effectuera les changements tout seul. Nous remercions notre réseau de confiance pour nous avoir suggéré cette idée.

Sous Windows 9x ou ME, on peut utiliser un fichier `.reg`, ce fichier contenant du texte est la description d'une branche de la base des registres. Lorsqu'on clique doublement dessus, cette branche de la base des registres sera automatiquement créée ou remplacée.

ATTENTION : cliquer doublement sur ce type de fichier ne demande pas de confirmation avant son exécution !

Pour Windows NT et 2000, il existe une commande `assoc` qui effectue de façon plus propre l'association désirée. Le plus simple est de l'ajouter dans le fichier `autoexec.bat` de façon à ce qu'elle soit exécuté par chaque utilisateur en début de session.

Le principe consiste à associer les extensions de fichiers correspondants à du code mobile à un exécutable qui ne fera rien de nuisible au système. *Notepad* est un bon candidat.

4 Solution

Pour Windows 9x et ME, le fichier `.reg` que vous construisez aura la forme suivante :

```
[HKEY_CLASSES_ROOT\VBSfile\Shell\Open\Command]
@="C:\\WINDOWS\\notepad.exe \"%1\" %*"
```

```
[HKEY_CLASSES_ROOT\VBSfile\Shell\Open2\Command]
@="C:\\WINDOWS\\Command\\notepad.exe \"%1\" %*"
```

Nota 1: les chemins logiques doivent correspondre à la configuration du système. Par exemple, si le système est installé sur le volume D:, les lignes 2 et 5 deviendront :

```
@="D:\\WINDOWS\\notepad.exe \"%1\" %*"
```

et

```
@="D:\\WINDOWS\\Command\\notepad.exe \"%1\" %*"
```

Nota 2: Les autres associations ne se font pas forcément de la même façon, les branches de la base des registres peuvent donc varier en fonction de la nouvelle association que vous y ferez.

Sous Windows NT, on ajoute à `autoexec.bat` la commande suivante :

```
assoc .vbs=txtfile
ou
assoc .js=txtfile
ou encore
assoc .wsh=txtfile
etc...
```

Gestion détaillée du document

19 octobre 2000 version initiale.