Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juin 2000
N° CERTA-2000-AVI-009

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Exécution de programmes locaux grâce aux fichiers d'aides de Windows

Gestion du document

Référence	CERTA-2000-AVI-009
Titre	Exécution de fichiers locaux grâce aux fichiers d'aides de Microsoft Windows
Date de la première version	20 juin 2000
Date de la dernière version	–
Source(s)	Avis CA-2000-12 du CERT/CC Bulletin 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 arbitraire de fichiers locaux.

2 Systèmes affectés

Tout système utilisant Microsoft Internet Explorer.

3 Résumé

Grâce à la lecture d'un fichier d'aide de Windows (extension .CHM) astucieusement construit, un utilisateur peut être conduit par une personne mal intentionnée à exécuter localement du code à son insu.

4 Description

Microsoft a proposé un format de fichiers d'aide pour Windows qui permet, en cliquant sur un lien, d'exécuter du code en local (programmes, ou scripts). Par exemple, en lisant l'aide de Windows pour configurer une imprimante, il est possible d'ouvrir le gestionnaire d'impression en cliquant sur un lien de cette aide.

Un utilisateur mal intentionné peut générer ce genre de fichier en y mettant des liens vers des fichiers exécutables locaux de son choix (voire vers des documents bureautique contenant des macros). Si ce fichier d'aide se trouve sur un lecteur réseau connecté (UNC) ou s'il est placé localement sur le disque (par détachement d'un mail, par exemple), il permet de faire exécuter des fichiers arbitraires par celui qui le lirait et cliquerait sur les liens insérés dans le texte. Il porfite du fait qu'en cliquant sur un lien on ne pense pas forcément exécuter du code.

Ce type de fichiers peut aussi être exécuté, de façon non-interactive, et donc à l'insu de l'utilisateur, via un contrôle ActiveX situé dans une page web ou dans un mail lu par Microsoft outlook.

5 Contournement provisoire

Il faut :

- Rester vigilant vis à vis des des documents de tout type contenant éventuellement des scripts (macro, VBS, ActiveX, etc.).
- Désactiver les contrôles ActiveX, comme indiqué dans les notes CERTA-2000-INF-002, CERTA-2000-AVI-002 et CERTA-2000-REC-001, pour les 4 types de Zones : Internet, Intranet Local, Sites de confiance (Maintenir une liste précise des sites utilisant HTTPS comme protocole), et Sites sensibles (Sites dont le contenu pourrait endomager votre système).
  Il existe une cinquième zone, qui n'est généralement pas visible appelée « Poste de travail » (My Computer). Les paramètres de sécurité pour cette zone sont observables ou modifiables par la base des registres (regedit).
  Pour plus de détails voir le site de microsoft :
  http://support.microsoft.com/support/kb/articles/Q182/569.asp
  En outre, les paramètres de sécurité de la zone poste de travail peuvent être administrés grâce au logiciel « Internet Explorer Administration Kit » (IEAK).
  Pour la version francaise :
  http://www.microsoft.com/windows/ieak/fr/download/default.asp

6 Solution

6.1 À la main

Le contrôle HHCtrl est le point central de l'exploitation de cette vulnérabilité. Si vous désirez agir plus finement (à vos risques et périls) que dans les recommandations générales des notes du CERTA, le CERT/CC propose de désactiver soit « Contrôles ActiveX reconnus sûrs pour l'écriture de scripts » soit les « Contrôles d'initialisation et de scripts ActiveX non marqués » uniquement pour le contrôle HHCtrl, qui sont tous les deux activés par défaut lors de l'installation d'Internet Explorer.

Pour celà, supprimez l'une des deux clefs suivantes de la base de registres :

- HKEY_CLASSES_ROOT\CLSID\{ADB880A6-D8FF-11CF-9377-00AA003B7A11}\Implemented Categories\{7DD95801-9882-11CF-9FA9-00AA006C42C4}
- HKEY_CLASSES_ROOT\CLSID\{ADB880A6-D8FF-11CF-9377-00AA003B7A11}\Implemented Categories\{7DD95802-9882-11CF-9FA9-00AA006C42C4}

6.2 correctif partiel

Microsoft fournit un correctif qui n'autorise pas l'exécution de code, par un lien situé dans un fichier d'aide de ce type, se trouvant sur un lecteur réseau. Ce correctif ne traite pas l'exécution de code si le fichier d'aide se trouve sur un disque local (suite à un télechargement par exemple) :

- Pour Internet explorer 4.0, 4.01, 5.0 et 5.01 sous Windows 95, 98 première et seconde édition et Windows NT4.0 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=210705
- Pour Internet Explorer 5.01 sous Windows2000
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=210706

Enfin, microsoft propose aussi un correctif pour outlook, protègeant un peu plus les utilisateurs de ce gestionnaire de courriers contre les scripts contenus dans les mails et les pièces jointes.

Pour le télecharger aller à l'adresse suivante :
http://www.officeupdate.com/2000/downloaddetails/out2ksec.htm

7 Documentation

- Bulletin de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms00-037.asp
  http://www.microsoft.com/technet/security/bulletin/fq00-037.asp
- Avis du CERT/CC :
  http://www.cert.org/advisories/CA-2000-12.html
- Modification des paramètres de la zone « poste de travail » par la base des registres
  http://support.microsoft.com/support/kb/articles/Q182/569.asp

Gestion détaillée du document

20 juin 2000 version initiale.