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 avril 2010
N° CERTA-2010-ALE-003-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft VBScript

Gestion du document

Référence	CERTA-2010-ALE-003-001
Titre	Vulnérabilité dans Microsoft VBScript
Date de la première version	02 mars 2010
Date de la dernière version	13 avril 2010
Source(s)	Avis Microsoft #981169 du 01 mars 2010 Avis CERTA-2010-AVI-170 du 14 avril 2010
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 à distance.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4;
- Microsoft Windows XP Service Pack 2 et Windows XP Service Pack 3;
- Microsoft Windows Server 2003 Service Pack 2.

3 Résumé

Une vulnérabilité dans VBScript permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance. L'éditeur a publié un correctif pour cette vulnérabilité

4 Description

Une vulnérabilité due à une faiblesse structurelle du format de fichier HLP permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

Le format HLP est le format historique utilisé pour les fichiers d'aide dans les environnements Microsoft. Il est remplacé depuis quelques années par le format CHM. Ce format de fichier est considéré comme non sûr car il permet l'execution de commandes arbitraires via des macros.

L'objet de cette alerte est qu'il est possible d'ouvrir ce type de fichiers HLP via Microsoft Internet Explorer en naviguant sur une page Web contenant du script. En effet, la fonction VBScript `MsgBox` permet l'ouverture de fichiers de type HLP, via une boîte de dialogue incitant l'utilisateur à appuyer sur la touche `F1`.

Le fichier HLP sera ouvert si et seulement si l'utilisateur appuie effectivement sur cette touche `F1`.

L'ouverture de ce fichier HLP permet alors l'execution de code à distance avec les privilèges de l'utilisateur courant.

Le fichier HLP peut se trouver sur le disque local, un partage SMB ou un serveur WEBDAV.

Il est à noter que du code d'exploitation est d'ores et déjà disponible sur Internet.

5 Contournement provisoire

En premier lieu, informer les utilisateurs de ne pas appuyer sur la touche `F1` lors de la navigation sur Internet.

Rappeler que les bonnes pratiques recommandent d'utiliser un compte utilisateur restreint pour la navigation sur Internet.

Côté contournement technique, il est possible de bloquer l'ouverture des fichiers HLP en modifiant les permissions de l'exécutable `winhlp32.exe` (voir la section contournement de l'avis Microsoft #981169)

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS10-022 du 13 avril 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-022.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-022.mspx
- Bulletin de sécurité Microsoft #981169 du 01 mars 2010 :
  http://www.microsoft.com/technet/security/advisory/981169.mspx
- Blog du MSRC Engineering du 01 mars 2010 :
  http://blogs.technet.com/srd/archive/2010/03/01/help-keypress-vulnerability-in-vbscript-enabling-remote-code-execution.aspx
- Document du CERTA CERTA-2010-AVI-170 du 14 avril 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-170/index.html
- Référence CVE CVE-2010-0483 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0483

Gestion détaillée du document

02 mars 2010 version initiale.

13 avril 2010 publication du correctif.