

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft VBScript

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-2010-AVI-170>

Gestion du document

Référence	CERTA-2010-AVI-170
Titre	Vulnérabilité dans Microsoft VBScript
Date de la première version	14 avril 2010
Date de la dernière version	–
Sources	Bulletin de sécurité Microsoft MS10-022 du 13 avril 2010 Alerte CERTA-2010-ALE-003 du 02 mars 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

VBScript 5.x sur :

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

3 Résumé

Une vulnérabilité dans VBScript, liée au format HLP, permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

4 Description

La fonction VBScript `MsgBox` permet l'ouverture de fichiers HLP par une boîte de dialogue incitant l'utilisateur à appuyer sur la touche F1. L'ouverture de ce fichier, local ou distant, permet alors l'exécution de code à distance avec les privilèges de l'utilisateur courant.

5 Solution

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

6 Documentation

- Document du CERTA CERTA-2010-ALE-003 du 02 mars 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-003/index.html>
- Bulletin de sécurité Microsoft MS10-022 du 13 avril 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-022.mspix>
<http://www.microsoft.com/technet/security/Bulletin/MS10-022.mspix>
- Référence CVE CVE-2010-0483 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0483>

Gestion détaillée du document

14 avril 2010 version initiale.