Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mai 2004
N° CERTA-2004-AVI-160

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le Centre d'Aide et de Support de Microsoft Windows

Gestion du document

Référence	CERTA-2004-AVI-160
Titre	Vulnérabilité dans le Centre d'Aide et de Support de Microsoft Windows
Date de la première version	12 mai 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS04-015 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 à distance.

2 Systèmes affectés

- Microsoft Windows XP ;
- Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition.

Les autres versions de Microsoft Windows ne sont pas affectées par cette vulnérabilité.

3 Résumé

Une vulnérabilité a été découverte dans le Centre d'Aide et de Support de certaines versions de Microsoft Windows.

4 Description

Le Centre d'Aide et de Support (`Help and Support Center`) est un service unifié permettant à l'utilisateur d'obtenir divers types d'assistance tels que l'accès aux informations du système ou à sa configuration. On peut y accéder à l'aide du protocole HCP (adresses réticulaires de type "hcp://").

Une vulnérabilité présente dans la gestion des liens réticulaires de type HCP permet à un individu mal intentionné d'exécuter du code arbitraire à distance à l'aide d'un site malicieux ou d'un message électronique malicieusement formé.

5 Contournement provisoire

- Désactiver l'utilisation du protocole HCP dans la base de registres :
  Effacer la clé `HKEY_CLASSES_ROOT\HCP` du registre ;
- mettre à jour les correctifs de sécurité, si vous utilisez Outlook 2000 Service Pack 1 ou les versions antérieures :
  http://www.microsoft.com/office/previous/outlook/2002security.asp
- ne lire et n'envoyer vos messages éléctoniques qu'au format texte :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/

6 Solution

Appliquer le correctif fourni par Microsoft (cf. Documentation).

Attention l'application des correctifs peut présenter certains problèmes si le Centre d'Aide et de Support est désactivé :
http://www.microsoft.com/default.asp?scid=kb;en-us;841996

7 Documentation

- Bulletin de sécurité #MS04-015 de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms04-015.mspx
- Référence CVE CAN-2004-0199 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0199

Gestion détaillée du document

12 mai 2004 version initiale.