Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 octobre 2003
N° CERTA-2003-AVI-169

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le protocole "Help and Support Center" de Microsoft

Gestion du document

Référence	CERTA-2003-AVI-169
Titre	Vulnérabilité dans le protocole "Help and Support Center" de Microsoft
Date de la première version	16 octobre 2003
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS03-044
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 avec les droits de l'utilisateur courant.

2 Systèmes affectés

- Microsoft Windows Me ;
- Microsoft Windows NT Workstation 4.0 ;
- Microsoft Windows NT Server 4.0 ;
- Microsoft Windows NT 4.0 Terminal Server Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Windows Server 2003.

3 Résumé

Une adresse réticulaire (*"URL"*) habilement conçue permet d'exécuter du code arbitraire lorsque l'utilisateur courant clique desssus. Les droits correspondent à ceux de ce dernier (Administrateur dans le cas d'une installation personnelle par défaut).

4 Description

"Help and Support Center" est un service unifié permettant à l'utilisateur d'obtenir divers types d'assistance. Il fournit par exemple de la documentation, l'accès à *"Windows Update"*, l'assistance de la compabilité matérielle... Il peut être accédé à l'aide d'adresses commençant par "hcp://" au lieu du classique "http://" du protocole HTTP. Bien que présent sur toutes les plateformes, il n'est en principe utilisable que depuis Windows XP.

Il existe un débordement de tampon dans un des composants du protocole HCP. Il permet à un utilisateur mal intentionné de faire exécuter du code arbitraire par le biais d'un message ou d'une page Internet au format HTML.

5 Contournement provisoire

Supprimer le support du protocole HCP dans la base de registre.

6 Solution

Appliquer le correctif fourni par Microsoft suivant la version du système d'exploitation (cf. Documentation).

7 Documentation

- Bulletin de sécurité MS03-044 de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms03-044.asp
- Référence CVE CAN-2003-0711 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0711

Gestion détaillée du document

16 octobre 2003 version initiale.