



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 février 2003
N° CERTA-2003-AVI-030

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole d'aide en ligne de Windows Millenium Edition

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-2003-AVI-030>

Gestion du document

Référence	CERTA-2003-AVI-030
Titre	Vulnérabilité du protocole d'aide en ligne de Windows Millenium Edition
Date de la première version	27 février 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS03-006 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.

2 Systèmes affectés

Windows Millenium Edition.

3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire au moyen d'un lien HTML astucieusement construit.

4 Description

Le centre d'aide et de support (*Help and Support Center*) de Microsoft permet aux utilisateurs d'obtenir de l'aide en ligne en suivant des liens commençant par `hcp://` au lieu de l'habituel `http://`.

Une vulnérabilité de type débordement de mémoire du protocole hcp sous Windows Millenium Edition permet à un utilisateur mal intentionné d'exécuter ou de lire des fichiers présents sur la machine de sa victime.

Le code arbitraire peut être exécuté si la victime clique sur une URL astucieusement construite placée sur un site web ou dans un message électronique.

5 Solution

Consulter le bulletin de sécurité MS03-006 de Microsoft (se référer au paragraphe Documentation) pour connaître la disponibilité des correctifs.

6 Documentation

- Bulletin de sécurité MS03-006 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS03-006.asp>
- Documentation additionnelle au bulletin de sécurité MS03-006 Microsoft :
http://www.microsoft.com/technet/security/security_Bulletin03-006.asp

Gestion détaillée du document

27 février 2003 version initiale.