



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 septembre 2002
N° CERTA-2002-AVI-211

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du Help Center de Windows XP

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-2002-AVI-211>

Gestion du document

Référence	CERTA-2002-AVI-211
Titre	Vulnérabilité du Help Center de Windows XP
Date de la première version	18 septembre 2002
Date de la dernière version	–
Source(s)	Base de connaissances de Microsoft Liste des correctifs apportés par le Service Pack 1
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

Destruction de fichiers.

2 Systèmes affectés

Windows XP.

3 Résumé

Une vulnérabilité du *Help Center* de Windows XP permet à un utilisateur mal intentionné de supprimer des fichiers du système de sa victime.

4 Description

Help Center (utilisant le protocole HCP) est un système d'aide à l'installation de nouveau matériel sous Windows XP. Lors de l'installation d'un nouveau périphérique, l'utilisateur est invité à remplir un formulaire afin de se procurer les pilotes adéquats.

Ce formulaire, stocké sur la machine victime, contient un `JScript` (Microsoft Java Script) permettant d'effacer des fichiers sur le système.

Un utilisateur mal intentionné peut supprimer des fichiers du système au moyen d'un lien habilement construit placé dans une page HTML, un e-mail, ou tout autre moyen d'afficher des liens cliquables.

5 Contournement Provisoire

Si vous n'utilisez pas la fonction *Help Center* qui consiste à remplir un formulaire envoyé à Microsoft pour obtenir les informations adéquates sur les périphériques que vous installez, supprimez le fichier nommé :

`\windows\PCHEALTH\HELPCTR\upldrvinfo.htm`

6 Solution

Appliquer le Service Pack 1 pour Windows XP qui corrige cette vulnérabilité :

<http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp>

7 Documentation

- Article Q328940 de la base de connaissances de Microsoft :
<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q328940>
- Liste des corrections effectuées par le Service Pack 1 pour Windows XP :
<http://support.microsoft.com/default.aspx?scid=/support/ServicePacks/Windows/XP/SP1FixListe.asp>

Gestion détaillée du document

18 septembre 2002 version initiale.