Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2010
N° CERTA-2010-ALE-008-004

**Affaire suivie par :**
CERTA

# BULLETIN D'ALERTE DU CERTA

**Objet : Vulnérabilité dans le Centre d'aide et de support Windows**

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-ALE-008`

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2010-ALE-008-004 |
| Titre | Vulnérabilité dans le Centre d'aide et de support Windows |
| Date de la première version | 10 juin 2010 |
| Date de la dernière version | 15 juillet 2010 |
| Source(s) | Avis de sécurité Microsoft #2219475 du 10 juin 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

Pour l'instant les systèmes suivants ont été identifiés comme vulnérables :

- Windows XP SP2/SP3 ;
- Windows 2003 SP2.

## 3 Résumé

Une vulnérabilité non-corrigée dans le `Centre d'aide et de support Windows` permet à un utilisateur distant malintentionné d'exécuter du code arbitraire.

# 4 Description

Une vulnérabilité non-corrigée a été découverte dans le `Centre d'aide et de support Windows`.

Elle permet à un utilisateur distant malintentionné d'exécuter du code arbitraire, notamment, via un navigateur internet.

Tous les navigateurs peuvent servir de vecteur d'exploitation, notamment si `Windows Media Player 9` est installé sur la machine. D'autres vecteurs d'exploitation sont potentiellement possibles, notamment les documents `Office`.

Des exemples de code d'exploitation de cette vulnérabilité sont d'ores et déjà recensés sur l'Internet. Cette vulnérabilité est actuellement activement exploitée.

Cette vulnérabilité concerne la gestion du protocole *HCP* utilisé par le `Centre d'aide et de support Windows` . Une lien *HCP* spécialement malformé permet ainsi l'exécution de code arbitraire à distance.

# 5 Contournements provisoires

Microsoft vient de publier un contournement sous la forme d'un paquet `FixIt` (voir section Documentation).

Si vous ne pouvez pas déployer ce paquet `FixIt`, et dans l'attente d'un correctif de l'éditeur, le CERTA recommande les mesures suivantes :

*Ces contournements peuvent avoir des effets de bord, notamment sur certaines fonctionnalités de l'aide de Windows.*

– Retirer les droits d'accès à l'exécutable HelpCtr.exe ;

```
Echo y| cacls %WINDIR%\PCHealth\HelpCtr\Binaries\HelpCtr.exe /E /P "Tout le monde":N
```

Pour désactiver ce contournement et autoriser l'accès à cet exécutable ;

```
Echo y| cacls %WINDIR%\PCHealth\HelpCtr\Binaries\HelpCtr.exe /E /R "Tout le monde"
```

– Modifier l'association du shell pour le protocole `HCP` ;
Renommer (ou supprimer) la clé de registre :

```
HKEY_CLASSES_ROOT\HCP\shell\open\command
```

Par exemple :

```
HKEY_CLASSES_ROOT\HCP\shell\open\_command
```

Le CERTA rappelle qu'il est recommandé de naviguer avec un compte utilisateur aux droits restreints et de désactiver l'interprétation de code dynamique (Javascript, ActiveX).

# 6 Solution

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

# 7 Documentation

– Bulletin de sécurité Microsoft MS10-042 du 13 juillet 2010 :
http://www.microsoft.com/france/technet/security/Bulletin/MS10-042.mspx
http://www.microsoft.com/technet/security/Bulletin/MS10-042.mspx
– Avis CERTA-2010-AVI-310 du 15 juin 2010 :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-310/
– Avis de sécurité Microsoft #2219475 du 10 juin 2010 :
http://www.microsoft.com/technet/security/advisory/2219475.mspx
– Microsoft FixIt KB2219475 du 11 juin 2010 :
http://support.microsoft.com/kb/2219475
– Référence CVE CVE-2010-1885 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1885

## Gestion détaillée du document

**10 juin 2010** version initiale ;

**11 juin 2010** avis de sécurité Microsoft #2219475 et modification des systèmes impactés, description et contournements ;

**14 juin 2010** modification des sections Contournement et Documentation pour l'ajout du FixIt ;

**5 juillet 2010** ajout de la référence CVE ;

**15 juillet 2010** ajout de la correction.