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-AVI-310

Affaire suivie par :
CERTA

AVIS DU CERTA

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

Gestion du document

Référence	CERTA-2010-AVI-310
Titre	Vulnérabilité dans le Centre d'aide et de support Windows
Date de la première version	15 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-042 du 13 juillet 2010 Alerte CERTA-2010-ALE-008 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

- 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 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 via des documents de formats divers envoyés en pièces jointes.

Cette vulnérabilité est activement exploitée sur l'Internet.

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 Solution

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

6 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
- Alerte CERTA-2010-ALE-008 du 10 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-008/
- Référence CVE CVE-2010-1885 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1885

Gestion détaillée du document

15 juillet 2010 version initiale.