Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 janvier 2005
N° CERTA-2005-AVI-010

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le composant ActiveX HTML Help

Gestion du document

Référence	CERTA-2005-AVI-010
Titre	Vulnérabilité dans le composant ActiveX `HTML Help`
Date de la première version	12 janvier 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-001
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Systèmes d'exploitation affectés par la vulnérabilité :

- Microsoft Windows 2000 Service Pack 3 & 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP 64-bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-bit version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 XP 64-bit Edition.

Systèmes également affectés par la vulnérabilité :

- Microsoft Internet Explorer 6.0 Service Pack 1 sous :
  - Microsoft Windows NT Server 4.0 Service Pack 6a ;
  - Microsoft Windows NT Server 4.0 Terminal Service Edition Service Pack 6.

3 Résumé

Une vulnérabilité découverte dans le composant ActiveX `HTML Help` permet à un utilisateur mal intentionné d'exécuter à distance du code arbitraire avec les privilèges de la victime.

4 Description

Le composant ActiveX `HTML Help` présente une vulnérabilité dans la gestion des *zones de contenus Web*. Cette vulnérabilité permet à une personne malveillante de porter atteinte à la confidentialité des données et/ou d'exécuter à distance du code arbitraire avec les privilèges de la victimes, grâce à un site web malicieusement constitué.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS05-001 du 11 janvier 2005 :
  http://www.microsoft.com/technet/security/bulletin/MS05-001.mspx
- Référence CVE CAN-2004-1043 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1043

Gestion détaillée du document

12 janvier 2005 version initiale.