

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans l'aide HTML de 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-2005-AVI-212>

---

### Gestion du document

Référence	CERTA-2005-AVI-212-001
Titre	Vulnérabilité dans l'aide HTML de Windows
Date de la première version	15 juin 2005
Date de la dernière version	17 juin 2005
Source(s)	Bulletin de sécurité Microsoft MS05-026
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

- Dénier de service ;
- exécution de code arbitraire.

## 2 Systèmes affectés

- Microsoft Windows 2000 SP3 et SP4 ;
- Microsoft Windows XP SP1 et SP2 ;
- Microsoft Windows XP édition 64-Bits SP1 (itanium) ;
- Microsoft Windows XP édition 64-Bits version 2003 (itanium) ;
- Microsoft Windows XP Professional édition 64 bits ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 SP1 ;
- Microsoft Windows Server 2003 (itanium) ;
- Microsoft Windows Server 2003 SP1 (itanium) ;
- Microsoft Windows 98 ;
- Microsoft Windows 98 seconde édition ;
- Microsoft Windows Millenium édition (ME).

### 3 Résumé

Une vulnérabilité présente dans le HTML Help de Windows peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire sur le système vulnérable.

### 4 Description

Une vulnérabilité est présente dans le HTML Help de Windows. Cette vulnérabilité peut être exploitée via une page au format HTML malicieusement construite permettant à un utilisateur mal intentionné d'exécuter du code sur la machine avec les privilèges de l'utilisateur ayant ouvert la session.

### 5 Contournement provisoire

Dans l'attente d'appliquer le correctif il est possible de désactiver le protocole HTML Help InfoTech (cf. bulletin de sécurité de l'éditeur, section documentation)

### 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 MS05-026 :  
<http://www.microsoft.com/france/technet/securite/ms05-026.msp>
- Référence CVE CAN-2005-1208 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1208>

### Gestion détaillée du document

**15 juin 2005** version initiale.

**17 juin 2005** mise à jour des systèmes affectés (ajout de Microsoft Windows 2000 SP4).