

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le composant ActiveX DHTML

---

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-059>

---

### Gestion du document

Référence	CERTA-2005-AVI-059
Titre	Vulnérabilité dans le composant ActiveX DHTML
Date de la première version	10 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-013 du 08 février 2005
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 à distance ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- 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 Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 pour systèmes Itanium.

## 3 Résumé

Une vulnérabilité découverte dans le composant ActiveX DHTML Help permet à un utilisateur mal intentionné d'exécuter à distance du code arbitraire sur le système vulnérable ou de porter atteinte à la confidentialité des données.

## 4 Description

Le composant ActiveX Dynamic HyperText Markup Language (DHTML) présente une vulnérabilité de type `cross-domain` qui permet à un individu mal intentionné de porter atteinte à la confidentialité des données du système vulnérable ou d'exécuter du code arbitraire avec les privilèges de la victime, au moyen d'une page ou d'un e-mail malicieusement contruit en HTML.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Microsoft MS05-013 du 08 février 2005 :  
<http://www.microsoft.com/technet/security/bulletin/MS05-013.msp>
- Référence CVE CAN-2004-1019 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1019>

## Gestion détaillée du document

10 février 2005 version initiale.