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 juin 2005
N° CERTA-2005-AVI-216

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des systèmes Microsoft Windows

Gestion du document

Référence	CERTA-2005-AVI-216
Titre	Vulnérabilité des systèmes Microsoft Windows
Date de la première version	15 juin 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-031 du 14 juin 2005
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

- Microsoft Windows 2000 Service Pack 3 et 4 ;
- Microsoft Windows XP Service Pack 1 et 2 ;
- Microsoft Windows XP édition 64-Bit Service Pack 1 (pour Itanium) ;
- Microsoft Windows XP édition 64-Bit Version 2003 (pour Itanium) ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 pour systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows 98, Windows 98 Seconde Edition, Windows Millenium Edition.

3 Résumé

Une vulnérabilité dans `Microsoft Step-By-Step Interactive Training` permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

4 Description

`Microsoft Step-By-Step Interactive Training` est un composant du système `Microsoft Windows` permettant l'exécution de tutoriels interactifs. Une vulnérabilité permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un signet de marque-pages (d'extension `.cbo`, `.cbl` ou `.cbm`) judicieusement construit.

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 MS05-031 du 14 juin 2005 :
  http://www.microsoft.com/technet/security/bulletin/MS05-031.mspx
- Référence CVE CAN-2005-1212 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1212

Gestion détaillée du document

15 juin 2005 version initiale.