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-011

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la gestion du format du curseur et des icônes

Gestion du document

Référence	CERTA-2005-AVI-011
Titre	Vulnérabilité dans la gestion du format du curseur et des icônes
Date de la première version	12 janvier 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-002
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.

2 Systèmes affectés

- Microsoft Windows 98 & 98 Second Edition ;
- Microsoft Windows Millennium Edition ;
- Microsoft Windows 2000 Service Pack 3 & 4 ;
- Microsoft Windows XP Service Pack 1 ;
- 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.
- 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 présente dans le traitement des formats d'icônes et de curseurs, permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de la victime.

4 Description

La vulnérabilité découverte permet à un utilisateur mal intentionné, au moyen d'un fichier au format d'icône ou de curseur malicieusement constitué d'exécuter du code arbitraire sur le système vulnérable, avec les droits de la victime. Cette vulnérabilité peut-être mise en œuvre grâce à une page web ou un message électronique malicieusement constitué.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS05-002 du 11 janvier 2005 :
  http://www.microsoft.com/technet/security/bulletin/MS05-002.mspx
- Référence CVE CAN-2004-1049 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1049
- Référence CVE CAN-2004-1305 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1305

Gestion détaillée du document

12 janvier 2005 version initiale.