



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 avril 2005
N° CERTA-2005-AVI-136

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'interpréteur de commandes 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-136>

Gestion du document

Référence	CERTA-2005-AVI-136
Titre	Vulnérabilité dans l'interpréteur de commandes Windows
Date de la première version	12 avril 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-016 du 12 avril 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 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows pour systèmes Itanium ;
- Microsoft Windows 98, Microsoft Windows 98 SE et Microsoft Windows Millenium Edition.

3 Résumé

Une vulnérabilité dans l'interpréteur de commandes Windows permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité dans la gestion de l'association d'un fichier à une application par l'interpréteur de commandes Windows a été découverte. Un utilisateur mal intentionné peut, par le biais d'un fichier malicieusement constitué, exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS05-016 du 12 avril 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-016.mspx>
- Référence CVE CAN-2005-0063 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0063>

Gestion détaillée du document

12 avril 2005 version initiale.