



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 09 février 2005
N° CERTA-2005-AVI-054

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-054>

Gestion du document

Référence	CERTA-2005-AVI-054
Titre	Vulnérabilité de l'interpréteur de commandes Windows
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-008 du 08 février 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 Server 2003 pour les systèmes Itanium.

3 Description

Une vulnérabilité affectant les événements de type « glisser-déposer » (drag and drop) sous Windows permet le téléchargement d'un fichier exécutable sur le système à l'insu de l'utilisateur. L'exploitation de cette vulnérabilité, par le biais d'un site web malicieusement constitué, permet l'exécution de code arbitraire à distance.

4 Solution

Appliquer le correctif de Microsoft tel qu'indiqué dans le bulletin de sécurité Microsoft MS05-008 du 08 février 2005 (voir section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS05-008 du 08 février 2005 :
<http://www.microsoft.com/technet/security/bulletin/ms05-008.msp>
- Référence CVE CAN-2005-0053 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053>

Gestion détaillée du document

09 février 2005 version initiale.