



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 juillet 2004
N° CERTA-2004-AVI-242

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-2004-AVI-242>

Gestion du document

Référence	CERTA-2004-AVI-242
Titre	Vulnérabilité dans l'interpréteur de commandes Windows
Date de la première version	15 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-024
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 NT Workstation 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Terminal Server Edition 4.0 Service Pack 6a ;
- Microsoft Windows 2000 Service Pack 2, Service Pack 3 et Service Pack 4 ;
- Microsoft Windows XP et XP Service Pack 1 ;
- 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 64-Bit Edition ;
- Microsoft Windows 98 et 98 SE ;
- Microsoft Windows Millennium Edition ;
- Internet Explorer 6.0 Service Pack 1 installé sur Windows NT 4.0 SP6a.

3 Résumé

Une vulnérabilité présente dans l'interpréteur de commandes de Microsoft Windows permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Un concepteur de site mal intentionné peut, en attirant un utilisateur sur une page judicieusement composée, exploiter une vulnérabilité présente dans l'interpréteur de commandes lors du lancement d'une application. Cette vulnérabilité entraîne l'exécution de code arbitraire avec les privilèges de l'utilisateur.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS04-024 du 13 juillet 2004 :
<http://www.microsoft.com/technet/security/bulletin/ms04-024.msp>
- Référence CVE CAN-2004-0420 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0420>

Gestion détaillée du document

15 juillet 2004 version initiale.