Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 avril 2003
N° CERTA-2003-AVI-077

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilité dans la gestion des messages par le noyau Windows**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2003-AVI-077 |
| Titre | Vulnérabilité dans la gestion des messages par le noyau Windows |
| Date de la première version | 17 avril 2003 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS03-13 |
| 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

Accès aux privilèges de l'administrateur (nécessite un compte sur la machine).

## 2 Systèmes affectés

- Microsoft Windows NT Workstation 4.0, NT Server 4.0 et NT Server 4.0 Terminal Server Edition ;
- Microsoft Windows 2000 Professional, Server et Advanced Server ;
- Microsoft Windows XP Professional et Home Edition.

## 3 Résumé

Une vulnérabilité dans la gestion des messages par le noyau Microsoft permet à un utilisateur mal intentionné possédant un compte sur la machine d'obtenir les droits de l'administrateur.

## 4 Description

Le noyau est le coeur d'un système d'exploitation chargé des tâches telles que la gestion des processus, la gestion de la mémoire, les accès aux périphériques, la gestion et la remontée des messages... Une vulnérabilité

dans la manière dont le noyau Microsoft gère les messages permet à un utilisateur mal intentionné possédant un compte sur la machine d'obtenir les droits de l'administrateur (création de comptes, configuration du système, effacement de données...).

# 5 Solution

Appliquer le correctif disponible sur le site de Microsoft :
http://support.microsoft.com/?id=811493

# 6 Documentation

- Bulletin de sécurité Microsoft MS03-13 :
  http://www.microsoft.com/technet/security/bulletin/MS03-013.asp
- Microsoft Knowledge Base Article 811493 :
  http://support.microsoft.com/?id=811493
- Référence CVE CAN-2003-0112 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0112

# Gestion détaillée du document

**17 avril 2003** version initiale.