Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2004
N° CERTA-2004-AVI-335

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service Microsoft NetDDE

Gestion du document

Référence	CERTA-2004-AVI-335
Titre	Vulnérabilité du service Microsoft NetDDE
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-031
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 Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 3 et Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP et Microsoft Windows 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 ;
- Microsoft Windows 98 Second Edition ;
- Microsoft Windows Millenium Edition.

Sur les systèmes Microsoft Windows Server 2003, Microsoft Windows 98, Microsoft Windows 98 Second Edition et Microsoft Windows Millenium Edition, le service NetDDE n'est pas activé par défaut.

3 Résumé

Une vulnérabilité du service NetDDE permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

4 Description

NetDDE (Network Dynamic Data Exchange) est un service qui permet à des applications de communiquer entre elles à travers un réseau.

Une vulnérabilité de type débordement de mémoire permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine.

5 Contournement provisoire

- Désactiver le service NetDDE ;
- ou bloquer les ports suivants : 135/udp, 137/udp, 138/udp, 445/udp, 135/tcp, 139/tcp, 445/tcp, 593/tcp.

6 Solution

Appliquer les correctifs fournis par Microsoft (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS04-031 du 12 octobre 2004 :
  http://www.microsoft.com/technet/security/bulletin/ms04-031.mspx
- Référence CVE CAN-2004-0206 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0206

Gestion détaillée du document

13 octobre 2004 version initiale.