Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 février 2001
N° CERTA-2001-AVI-014

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'agent NDDE de Microsoft Windows

Gestion du document

Référence	CERTA-2001-AVI-014
Titre	Vulnérabilité de l'agent NDDE de Microsoft Windows
Date de la première version	07 février 2001
Date de la dernière version	–
Source(s)	bulletin de sécurité Microsoft
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

Élévation de privilèges.

2 Systèmes affectés

Tout système Microsoft Windows connecté à Internet ou à un intranet comprenant des systèmes sous Windows 2000.

3 Résumé

Une vulnérabilité de l'agent NDDE (*Network Dynamic Data Exchange*) permet à un utilisateur mal intentionné d'élever ses privilèges et d'exécuter ainsi des commandes et des programmes auxquels il n'aurait normalement pas accès.

4 Description

NDDE est un service de Windows permettant le partage d'informations et de données d'applications entre plusieurs machines distantes.

Dans toutes les versions de Windows qui précédent Windows 2000, l'agent NDDE fonctionne avec les privilèges de l'utilisateur, ce qui limite les possibilités d'exécutions de commandes de ce dernier uniquement à celle qui lui sont autorisées. De plus si un partage de données est installé sur une machine, l'agent NDDE aura pour règles de sécurités celles qui s'appliquent à l'utilisateur local de cette machine.

Sous Windows 2000, cet agent fonctionne avec les privilèges du système (*Local System*). Une mauvaise gestion des limites d'action de NDDE permet à un utilisateur d'exécuter des commandes avec les privilèges du système. Si la machine victime est un serveur de domaine, il peut prendre possession du domaine entier.

5 Contournement provisoire

En règle générale, il ne faut pas laisser des utilisateurs sans privilège accéder localement à un serveur ou les autoriser à y exécuter du code à distance (rcmd, NDDE, etc.). Si cette règle est appliquée, elle limitera nettement les dégâts possibles de ce type de vulnérabilités.

6 Solution

Appliquer le correctif de Microsoft pour Windows 2000 présent à l'adresse suivante :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=27526

7 Documentation

- L'avis et la FAQ de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms01-007.asp
  http://www.microsoft.com/technet/security/bulletin/fq01-007.asp
- La base de connaissances de Microsoft concernant NDDE :
  http://support.microsoft.com/support/kb/articles/Q114/0/89.asp

Gestion détaillée du document

07 février 2001 version initiale.