Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2004
N° CERTA-2004-AVI-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Data Access Components

Gestion du document

Référence	CERTA-2004-AVI-006
Titre	Vulnérabilité de Microsoft Data Access Components
Date de la première version	14 janvier 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS04-003
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 Data Access Components version 2.5 (inclus avec Microsoft Windows 2000) ;
- Microsoft Data Access Components version 2.6 (inclus avec Microsoft SQL Server 2000) ;
- Microsoft Data Access Components version 2.7 (inclus avec Microsoft Windows XP) ;
- Microsoft Data Access Components version 2.8 (inclus avec Microsoft Windows Server 2003).
- Microsoft Data Access Components version 2.8 (inclus avec Microsoft Windows Server 2003 64-Bit Edition).

3 Résumé

Une vulnérabilité dans Microsoft Data Access Components (MDAC) permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système.

4 Description

MDAC permet d'effectuer de nombreuses opérations sur les bases de données : se connecter à une base de données, récupérer des données, ...

Lorsqu'un client recherche la liste des serveur SQL présents sur son réseau, il envoie une requête en diffusion (broadcast) à toutes les machines du réseau.

Une vulnérabilité présente dans le traitement des réponses à cette requête peut être exploitée par un utilisateur mal intentionné pour provoquer un débordement de mémoire.

Il est alors possible pour l'attaquant d'exécuter du code arbitraire sur la machine avec les privilèges de l'application ayant lancé la requête en diffusion.

5 Solution

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

6 Documentation

Bulletin de sécurité MS04-003 de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS04-003.asp

Gestion détaillée du document

14 janvier 2004 version initiale.