

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Data Access Components

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-2003-AVI-140>

Gestion du document

Référence	CERTA-2003-AVI-140
Titre	Vulnérabilité de Microsoft Data Access Components
Date de la première version	21 août 2003
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS03-033
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 ;
- élévation de privilèges.

2 Systèmes affectés

Microsoft Data Access Components (MDAC) versions 2.5, 2.6 et 2.7. La version 2.8 n'est pas vulnérable.

MDAC est installé par défaut sur les systèmes suivants :

- Microsoft Windows XP ;
- Microsoft Windows 2000 ;
- Microsoft Windows Millenium Edition ;
- Microsoft Windows Server 2003.

La version installée sur Windows Server 2003 n'est pas vulnérable.

3 Résumé

Une vulnérabilité de type débordement de mémoire 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

Appliquer le correctif proposé par Microsoft.

6 Documentation

Avis de sécurité Microsoft MS03-033 :

<http://www.microsoft.com/technet/security/bulletin/MS03-033.asp>

Gestion détaillée du document

21 août 2003 version initiale.