

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans MDAC pour Microsoft SQL Server

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-2002-AVI-164>

Gestion du document

Référence	CERTA-2002-AVI-164
Titre	Débordement de mémoire dans MDAC pour Microsoft SQL Server
Date de la première version	01 août 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS02-040 de 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

- Débordement de mémoire ;
- exécution de code arbitraire.

2 Systèmes affectés

Tout serveur sous Microsoft SQL Server 7.0 ou 2000 sur lequel est installé MDAC (Microsoft Data Access Components) versions 2.5 SP2 et antérieures, 2.6 SP2 et antérieures et 2.7 Gold et antérieures.

3 Résumé

Un débordement de mémoire présent dans Microsoft MDAC, installé par défaut sur les serveurs Microsoft SQL Server, permet à un utilisateur mal intentionné de provoquer un débordement de mémoire et, dans certaines conditions, l'exécution de code arbitraire.

4 Description

Microsoft MDAC (Microsoft Data Access Components) fournit des fonctions pour exploiter une base de données Microsoft SQL Server. Un utilisateur mal intentionné peut envoyer une requête mal formée à ce module qui provoque un débordement de mémoire tampon conduisant, dans certains cas, à l'exécution de code arbitraire sur le serveur. Ce code sera exécuté avec les privilèges de l'application SQL Server. Dans le cas d'une installation standard, il s'agira des droits d'un utilisateur du domaine. L'utilisateur mal intentionné pourra, entre autre, modifier, ajouter et effacer des données dans la base.

Le module MDAC est fourni dans de nombreuses applications de Microsoft Windows mais seuls les serveurs SQL sont vulnérables.

Pour connaître la version de MDAC installée sur votre système, examinez la clé suivante dans la base de registre de votre serveur :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess.
```

La clé `FullInstallVer` vous fournit une valeur de type `x.xx.yyyy.y` où `x.xx` correspond à la version de MDAC installée.

5 Solution

Installez le correctif correspondant à votre version de MDAC. Ce correctif est disponible en téléchargement sur le site Web de Microsoft (cf la section Documentation).

6 Documentation

Bulletin de sécurité #MS02-040 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS02-040.asp>

Gestion détaillée du document

01 août 2002 version initiale.