



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 novembre 2002  
N° CERTA-2002-AVI-249

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des composants MDAC sous Microsoft Windows

---

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-249>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2002-AVI-249                                       |
| Titre                       | Vulnérabilité des composants MDAC sous Microsoft Windows |
| Date de la première version | 21 novembre 2002   |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité MS02-065 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

- Exécution de code arbitraire ;
- déni de service uniquement sur les outils URLScan.

## 2 Systèmes affectés

- Microsoft Data Access Component 2.1 ;
- Microsoft Data Access Component 2.5 ;
- Microsoft Data Access Component 2.6 ;
- Internet Explorer 5.01 ;
- Internet Explorer 5.5 ;
- Internet Explorer 6.0.

Nota :

- Remote Data Services (RDS) n'est pas activé par défaut lors de l'installation d'Internet Information Server (IIS).

Mais les serveurs IIS qui utilisent une version affectée de Microsoft Data Access Component MDAC et ayant activé RDS sont vulnérables.

- MDAC est installé et RDS activé par défaut sur les clients Internet Explorer. Actuellement, il n'est pas possible de le désactiver.
- Sous Windows XP, la version 2.7 de MDAC est installée. Cette vulnérabilité n'affecte donc pas les systèmes sous Windows XP.
- Selon Microsoft les outils URLScan ne devraient pas permettre l'exécution de code arbitraire mais il est possible de bloquer le système à distance au moyen de la vulnérabilité décrite dans cet avis.

### 3 Résumé

Il est possible d'exécuter du code arbitraire à distance en effectuant une requête RDS utilisée par les composants MDAC installés sur une machine cible.

### 4 Description

MDAC (Microsoft Data Access Components) fournit des fonctions pour exploiter des bases de données, comme connecter plusieurs bases de données entre elles, ou renvoyer des réponses à un client, etc.

RDS (Remote Data Services) est un des composants de MDAC qui permet à un client d'accéder à des bases de données à travers une interface web.

Les navigateurs Internet Explorer possèdent un client MDAC installé avec le client RDS activé par défaut.

La fonction nommée *RDS Data Stub* permet d'interpréter des requêtes HTML et de les transformer en requêtes RDS pour les transmettre à une base de données.

Une vulnérabilité de *RDS Data Stub* permet à un utilisateur mal intentionné d'effectuer une attaque de type débordement de mémoire à distance.

Il peut ainsi exécuter du code arbitraire à distance au moyen d'une requête RDS effectuée à travers une URL astucieusement construite et dirigée vers un serveur web possédant MDAC avec RDS activé.

La même attaque peut être effectuée contre un client Internet Explorer en incluant une réponse HTTP habilement construite dans une page web ou dans un message au format HTML.

URLScan est un outil du paquetage IISLockdown (servant à renforcer la sécurité des serveurs web IIS) de Microsoft qui permet de journaliser et/ou de bloquer les attaques par le biais d'URL habilement construites. Les URL passent dans un filtre ASCII avant d'être transférées et traitées par le serveur web.

Par conséquent il est impossible d'exécuter un binaire au moyen de cette attaque au travers des filtres d'URLScan. Cependant elle aura pour conséquence un déni de service en bloquant la machine victime.

### 5 Solution

Consulter le bulletin de sécurité MS02-065 de Microsoft (voir paragraphe documentation) pour connaître la disponibilité des correctifs à appliquer.

### 6 Documentation

Bulletin de sécurité MS02-065 de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/MS02-065.asp>

### Gestion détaillée du document

21 novembre 2002 version initiale.