

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur la fonction Microsoft Data Access Components (MDAC)

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-2006-AVI-151>

Gestion du document

Référence	CERTA-2006-AVI-151
Titre	Vulnérabilité sur la fonction Microsoft Data Access Components (MDAC)
Date de la première version	12 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-014
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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Windows XP Service Pack 1 exécutant Microsoft Data Access Components 2.7 Service Pack 1 ;
- Microsoft Windows XP Service Pack 2 exécutant Microsoft Data Access Components 2.8 Service Pack 1 ;
- Microsoft Windows XP Professionnel Edition 64 bits exécutant Microsoft Data Access Components 2.8 Service Pack 2 ;
- Microsoft Windows Server 2003 exécutant Microsoft Data Access Components 2.8 ;
- Microsoft Windows Server 2003 Service Pack 1 pour systèmes Itanium exécutant Microsoft Data Access Components 2.8 ;
- Microsoft Windows Server 2003 pour systèmes Itanium exécutant Microsoft Data Access Components 2.8 Service Pack 2 ;
- Microsoft Windows Server 2003 Edition 64 bits exécutant Microsoft Data Access Components 2.8 Service Pack 2 ;

3 Résumé

Une vulnérabilité présente dans le contrôle ActiveX RDS.Dataspace distribué par Microsoft Data Access Components, peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire à distance.

4 Description

RDS (Remote Data Service) est une fonctionnalité d'ADO (ActiveX Data Object) distribué par MDAC Microsoft Data Access Components.

RDS est utilisé pour déplacer des données d'un serveur vers une application client ou vers une page web.

Une vulnérabilité est présente dans l'ActiveX RDS.Dataspace. Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné, via un site web construit de façon malveillante, pour exécuter du code arbitraire ou réaliser un déni de service sur le poste de l'utilisateur parcourant ce site web.

5 Contournement provisoire

- Configurer Internet Explorer de façon à ne pas autoriser automatiquement le téléchargement et l'exécution des contrôles ActiveX ;
- Désactiver le contrôle ActiveX RDS.Dataspace.

6 Solution

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

7 Documentation

- Bulletin de sécurité Microsoft MS06-014 du 11 avril 2006 :
<http://www.microsoft.com/france/technet/securite/MS06-014.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-014.msp>
- Référence CVE CVE-2006-003 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-003>

Gestion détaillée du document

12 avril 2006 version initiale.