Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 septembre 2003
N° CERTA-2003-AVI-148

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Access Snapshot Viewer

Gestion du document

Référence	CERTA-2003-AVI-148
Titre	Vulnérabilité dans Microsoft Access Snapshot Viewer
Date de la première version	04 septembre 2003
Date de la dernière version	–
Source(s)	Microsoft Security Bulletin MS03-038
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.

2 Systèmes affectés

- Microsoft Access 97 ;
- Microsoft Access 2000 ;
- Microsoft Access 2002 ;
- Microsoft Access Snapshot Viewer (téléchargeable).

3 Résumé

Une vulnérabilité de type débordement de mémoire permet l'exécution de code arbitraire sur une machine possédant Microsoft Access Snapshot Viewer, par le biais d'un site web malicieusement construit.

4 Description

Microsoft Access Snapshot Viewer permet de visualiser un aperçu instantané d'une base de données Access, sans avoir installé l'ensemble du logiciel Microsoft Access.

Microsoft Access Snapshot Viewer est présent dans toutes les versions d'Access, même s'il n'est pas installé par défaut. Il peut également être téléchargé séparément.

Microsoft Access Snapshot Viewer utilise un contrôle ActiveX, dont une des fonctions comporte une vulnérabilité de type débordement de mémoire.

Un utilisateur mal intentionné peut créer une page web faisant malicieusement appel au contrôle ActiveX vulnérable, et inciter une victime potentielle à s'y rendre. Il pourra dans ce cas exécuter du code arbitraire sur la machine, avec les privilèges de l'utilisateur victime.

5 Solution

Appliquer le correctif fourni par Microsoft (cf. Documentation).

6 Documentation

Avis de sécurité Microsoft MS03-038:
http://www.microsoft.com/technet/security/bulletin/ms03-038.asp

Gestion détaillée du document

04 septembre 2003 version initiale.