

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Access Snapshot Viewer

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-2008-ALE-009>

Gestion du document

Référence	CERTA-2008-ALE-009-001
Titre	Vulnérabilité dans Microsoft Access Snapshot Viewer
Date de la première version	08 juillet 2008
Date de la dernière version	13 août 2008
Source(s)	Bulletin Microsoft 955179 du 07 juillet 2008
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.

2 Systèmes affectés

- Snapshot Viewer for Microsoft Access ;
- Microsoft Office Access 2000 ;
- Microsoft Office Access XP ;
- Microsoft Office Access 2003.

3 Résumé

Une vulnérabilité dans le contrôle *ActiveX* du *Snapshot Viewer for Microsoft Access* permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été identifiée dans le contrôle *ActiveX snapview.ocx* de *Snapshot Viewer for Microsoft Access*. Celle-ci peut être exploitée par une personne malintentionnée qui peut ainsi télécharger des fichiers dans des répertoires arbitraires d'une machine vulnérable, en incitant la victime à visiter une page web spécialement conçue.

Le contrôle *ActiveX* est signé par *Microsoft* et installé par défaut avec les versions 2000, XP, et 2003 de *Microsoft Office Access*.

La vulnérabilité est actuellement exploitée.

5 Contournement provisoire

Le contrôle *ActiveX* vulnérable peut être désactivé dans la base de registre :

Exécuter `regedit.exe`, puis accéder à la clé suivante :

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{F0E42D50-368C-11D0-AD81-00A0C90DC8D9}` et mettre la valeur « Compatibility Flags » à 00000400.

Faire de même pour les CLSID suivants :

`{F0E42D60-368C-11D0-AD81-00A0C90DC8D9}`
`{F2175210-368C-11D0-AD81-00A0C90DC8D9}`

Le CERTA recommande également les actions suivantes :

- utiliser un navigateur alternatif tel que *Mozilla Firefox*, *Opera*, *Safari*, *Kmeleon*, etc.;
- mettre à jour vers *Internet Explorer 7*, cocher le choix « Demander » dans l'option « Exécuter les contrôles ActiveX et les plugins », ou désactiver l'exécution des contrôles *ActiveX* ;
- naviguer en utilisant un compte d'utilisateur aux droits limités ;
- naviguer sur des sites de confiance.

6 Solution

Se référer au bulletin de sécurité MS08-041 de Microsoft pour l'obtention des correctifs (cf. section Documentation). Ce dernier est présenté dans l'avis CERTA-2008-AVI-413.

7 Documentation

- Avis du CERTA CERTA-2008-AVI-413 du 13 août 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-413/>
- Bulletin de sécurité Microsoft 955179 du 07 juillet 2008 :
<http://www.microsoft.com/technet/security/advisory/955179.msp>
- Note de vulnérabilité de l'US-CERT VU#837785 du 07 juillet 2008 :
<http://www.kb.cert.org/vuls/id/837785>
- Référence CVE CVE-2008-2463 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2463>

Gestion détaillée du document

08 juillet 2008 version initiale.

13 août 2008 publication du correctif par Microsoft.