Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juin 2007
N° CERTA-2007-AVI-082-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Microsoft concernant un objet OLE associé à un fichier RTF

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-2007-AVI-082

Gestion du document

Référence	CERTA-2007-AVI-082-001
Titre	Vulnérabilités de Microsoft concernant un objet OLE associé à un fichier RTF
Date de la première version	14 février 2007
Date de la dernière version	13 juin 2007
Source(s)	Bulletins de sécurité Microsoft MS07-011, MS07-012 et MS07-013 du 13 février 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003, y compris le Service Pack 1 ;
- Microsoft Windows Server 2003, y compris le Service Pack 1, pour les systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition.
- Microsoft Office 2000 Service Pack 3 ;
- Microsoft Office 2000 Service Pack 2 ;
- Microsoft Office 2000 Packs Multilangues ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Project 2000 Service Release 1 ;
- Microsoft Project 2002 Service Pack 1 ;
- Microsoft Learning Essentials 1.0, 1.1 et 1.5 pour Microsoft Office ;

– Microsoft Visual Studio .NET 2002 ;
– Microsoft Visual Studio .NET 2002 Service Pack 1 ;
– Microsoft Visual Studio .NET 2003 ;
– Microsoft Visual Studio .NET 2003 Service Pack 1.

3 Description

Plusieurs vulnérabilités ont été identifiées dans les produits Microsoft, relatives à l'interprétation d'un objet `OLE` dans un fichier au format `RTF` (pour *Rich Text Format*).

Un objet `OLE` (pour *Object Linking and Embedding*) permet à une application de dialoguer avec d'autres, bien qu'elles manipulent des formats différents. Plusieurs vulnérabilités ont été identifiées liées à l'utilisation de tels objets via des fichiers au format `RTF` (pour *Rich Text Format*). `RTF` est reconnu par la majorité des logiciels de traitement de texte actuels.

Les vulnérabilités concernent :

1. les composants `OLE Dialog` de Microsoft Windows ne manipuleraient pas correctement les objets `OLE` insérés dans les fichiers `RTF`, pouvant provoquer un débordement de mémoire ;
2. les classes *Microsoft Foundation Classes* (`MFC`) fournies par Microsoft Windows et Visual Studio, et permettant de manipuler les objets `OLE`, n'interpréteraient pas correctement les objets `OLE` insérés dans les fichiers `RTF` ;
3. les composants `RichEdit` de Windows et Office ne manipuleraient pas correctement les fichiers `RTF` contenant des objets `OLE`.

Chaque vulnérabilité peut être exploitée par une personne malveillante qui construirait de manière particulière un fichier d'extension `.rtf`. Une personne qui ouvrirait ce dernier (téléchargement sur une page Internet, ou comme pièce jointe à un courrier électronique par exemple), provoquerait l'exécution de code arbitraire sur sa machine vulnérable.

4 Solution

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

5 Documentation

– Bulletin de sécurité Microsoft MS07-011 du 13 février 2007 :
http://www.microsoft.com/france/technet/security/bulletin/MS07-011.mspx
http://www.microsoft.com/technet/security/Bulletin/MS07-011.mspx
– Bulletin de sécurité Microsoft MS07-012 du 13 février 2007, mis à jour le 12 juin 2007 :
http://www.microsoft.com/france/technet/security/bulletin/MS07-012.mspx
http://www.microsoft.com/technet/security/Bulletin/MS07-012.mspx
– Bulletin de sécurité Microsoft MS07-013 du 13 février 2007 :
http://www.microsoft.com/france/technet/security/bulletin/MS07-013.mspx
http://www.microsoft.com/technet/security/Bulletin/MS07-013.mspx
– Référence CVE CVE-2006-1311 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1311
– Référence CVE CVE-2007-0025 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0025
– Référence CVE CVE-2007-0026 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0026

Gestion détaillée du document

14 février 2007 version initiale.
13 juin 2007 mise à jour du bulletin de sécurité Microsoft MS07-012 du 12 juin 2007.