Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2007
N° CERTA-2007-AVI-081

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du moteur de protection mpengine.dll de 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-2007-AVI-081

Gestion du document

Référence	CERTA-2007-AVI-081
Titre	Vulnérabilité du moteur de protection mpengine.dll de Microsoft Windows
Date de la première version	14 février 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-010 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

- Windows Live OneCare ;
- Microsoft Antigen pour Exchange 9.x ;
- Microsoft Antigen pour SMTP Gateway 9.x ;
- Microsoft Windows Defender ;
- Microsoft Windows Defender x64 Edition ;
- Microsoft Windows Defender pour Windows Vista ;
- Microsoft Forefront Security pour Exchange Server ;
- Microsoft Forefront Security pour SharePoint.

3 Description

Une vulnérabilité, de type débordement d'entier, a été identifiée dans le moteur de protection contre les codes malveillants (`mpengine.dll`) fourni avec certaines applications de sécurité Microsoft. Celle-ci se produirait au cours de l'analyse de documents au format `PDF` (pour *Portable Document Format*).

Une personne malveillante pourrait construire un fichier d'extension `.pdf` exploitant cette vulnérabilité. Si une personne récupère ce dernier (soit en le téléchargeant via une page Web, soit comme pièce jointe d'un courrier électronique par exemple), du code malveillant pourrait être exécuté lorsque l'antivirus de Mirosoft analyserait le fichier.

4 Solution

Se référer au bulletin de sécurité MS07-010 de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS07-010 du 13 février 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/MS07-010.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-010.mspx
- Référence CVE CVE-2006-5270 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5270

Gestion détaillée du document

14 février 2007 version initiale.