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 mai 2008
N° CERTA-2008-ALE-005-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Jet Database Engine

Gestion du document

Référence	CERTA-2008-ALE-005-002
Titre	Vulnérabilité dans Microsoft Jet Database Engine
Date de la première version	25 mars 2008
Date de la dernière version	14 mai 2008
Source(s)	Bulletin de sécurité Microsoft #950627 du 21 mars 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

Les versions suivantes de *Microsoft* Word sont affectées :
- Word 2000 Service Pack 3 ;
- Word 2002 Service Pack 3 ;
- Word 2003 Service Pack 2 ;
- Word 2003 Service Pack 3 ;
- Word 2007 ;
- Word 2007 Service Pack 1.

Seuls les systèmes d'exploitation Microsoft Windows 2000 Service Pack 4, Windows XP Service Pack 2, et Windows Server 2003 Service Pack 1 sont concernés. Les versions de *Microsoft* Jet Database Engine affectées sont antérieures à 4.0.9505.0 (`Msjet40.dll`).

3 Résumé

Une vulnérabilité dans *Microsoft* Jet Database Engine permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire affecte *Microsoft* Jet Database Engine. Elle permet à une personne malintentionnée d'exécuter du code arbitraire à distance avec les droits de l'utilisateur. Cette faille semble être ancienne, toutefois elle n'a pas été corrigée par *Microsoft* car l'éditeur ne considère pas le format `mdb` (*Microsoft* Access) comme un format sûr (comme les fichiers *exe*, *bat*, *cmd* par exemple). Ainsi, ce type de fichier est par exemple automatiquement bloqué dans *Microsoft* Outlook (voir KB#925330).

Cependant, il a récemment été montré que la vulnérabilité de `Msjet40.dll` dont fait l'objet cet avis peut toutefois être exploitée via l'ouverture d'un fichier au format `doc`, qui appelle à son tour un fichier `mdb` spécifiquement construit.

Plusieurs cas d'exploitations ont d'ores et déjà été signalés à *Microsoft*.

Mise à jour du 14 mai 2008 :

Cette vulnérabilité est corrigée et mentionnée dans le bulletin *Microsoft* MS08-044 publié le 13 mai 2008. Ce dernier est détaillé dans l'avis CERTA-2008-AVI-244.

5 Contournement provisoire

Dans l'attente d'un correctif, plusieurs mesures permettent de réduire l'impact de l'exploitation de cette vulnérabilité :

- utiliser un compte aux droits restreints ;
- utiliser un logiciel de traitement de texte alternatif ;
- n'ouvrir que des documents de confiance ;
- être circonspect à l'égard des pièces jointes de courriels.

Il est également possible de désactiver le *Microsoft* Jet Database Engine en exécutant la commande suivante :

```
echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /P everyone:N
```

Ceci a pour effet de restreindre l'accès au fichier `msjet40.dll` à tous les utilisateurs. Les applications faisant appel à *Microsoft* Jet Database Engine risquent de ne plus fonctionner.

Pour restaurer un accès normal à ce fichier, exécuter :

```
echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /R everyone
```

6 Solution

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

7 Documentation

- Document du CERTA CERTA-2008-AVI-244 du 14 mai 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-244/index.html
- Bulletin de sécurité Microsoft MS08-028 du 13 mai 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-028.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-028.mspx
- Bulletin de sécurité Microsoft #950627 du 21 mars 2008 :
  http:///www.microsoft.com/technet/security/advisory/950627.mspx
- Article décrivant les fichiers non sûrs :
  http://support.microsoft.com/kb/925330
- Entrée du 24 mars 2008 dans le bloc-notes du MSRC :
  http://blogs.technet.com/msrc/archive/2008/03/24/update-msrc-blog-microsoft-security-advisory-950627.aspx

- Référence CVE CVE-2008-1092 :
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1092
- Bulletin de sécurité de l'US-CERT VU#936529
  http://www.kb.cert.org/vuls/id/936529

Gestion détaillée du document

25 mars 2008 version initiale.

26 mars 2008 correction d'un lien, ajout d'un contournement provisoire et de la référence au bulletin de l'US CERT.

14 mai 2008 publication du correctif par l'éditeur.