Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 avril 2009
N° CERTA-2008-ALE-015-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le convertisseur de texte WordPad

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-015

Gestion du document

Référence	CERTA-2008-ALE-015-001
Titre	Vulnérabilité dans le convertisseur de texte de WordPad
Date de la première version	10 décembre 2008
Date de la dernière version	15 avril 2009
Source(s)	Bulletin de sécurité Microsoft #960906 du 09 décembre 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

- WordPad Text Converter sur Windows 2000 Service Pack 4 ;
- WordPad Text Converter sur Windows XP Service Pack 2 ;
- WordPad Text Converter sur Windows 2003 Service Pack 1 ;
- WordPad Text Converter sur Windows 2003 Service Pack 2.

3 Résumé

Une vulnérabilité dans *WordPad Text Converter* permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité dans *WordPad Text Converter* permet à une personne malintentionnée distante d'exécuter du code arbitraire en incitant une personne à ouvrir un fichier *Word 97* spécialement conçu. L'utilisation de *WordPad* peut être forcée même si *Microsoft Office Word* est installé, au moyen, par exemple, d'un fichier d'extension `.wri`.

L'éditeur affirme que cette vulnérabilité est actuellement exploitée.

Cette vulnérabilité n'affecte pas les utilisateurs de *Windows XP Service Pack 3*, *Windows Vista*, et *Windows 2008*.

5 Contournement provisoire

Les utilisateurs de *Windows XP Service Pack 2* doivent mettre à jour leur système en *Service Pack 3*.

Il est possible de désactiver le convertisseur de texte de *WordPad* avec la commande suivante en ligne de commande :

```
echo y| cacls "%ProgramFiles%\Windows NT\Accessories\mswrd8.wpc" /E /P everyone:N
```

Pour réactiver le convertisseur de texte, changer le propriétaire du fichier `mswrd8.wpc` à « Administrateurs » (cf. bulletin de sécurité Microsoft) et taper la commande suivante :

```
echo y| cacls "%ProgramFiles%\Windows NT\Accessories\mswrd8.wpc" /E /R everyone
```

Les administrateurs peuvent également filtrer les fichiers de type `.wri` pour empêcher l'utilisation automatique de *WordPad*.

Enfin, le CERTA rappelle quelques bonnes pratiques :

- utiliser un compte utilisateur aux droits restreints ;
- n'ouvrir que des documents provenant de sources de confiance ;

6 Solution

Se référer au bulletin de sécurité MS09-010 de Microsoft pour l'obtention des correctifs (cf. section Documentation). Le CERTA a publié l'avis CERTA-2009-AVI-140 à ce sujet.

7 Documentation

- Bulletin de sécurité Microsoft 960906 du 09 décembre 2008 :
  http://www.microsoft.com/technet/security/advisory/960906.mspx
- Référence CVE CVE-2008-4841 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4841
- Avis du CERTA CERTA-2009-AVI-140 du 15 avril 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-140/
- Bulletin de sécurité Microsoft MS09-010 du 14 avril 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-010.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-010.mspx

Gestion détaillée du document

10 décembre 2008 version initiale.

15 avril 2009 ajout des références au bulletin de sécurité Microsoft MS09-010.