



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-2009-AVI-140

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les convertisseurs de texte WordPad et Office

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-2009-AVI-140>

Gestion du document

Référence	CERTA-2009-AVI-140
Titre	Vulnérabilités dans les convertisseurs de texte WordPad et Office
Date de la première version	15 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-010 du 14 avril 2009
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

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et 3 ;
- Microsoft Windows XP Professional Edition x64, Service Pack 2 compris ;
- Microsoft Windows Server 2003 Service Pack 1 et 2, y compris les versions pour systèmes x64 et Itanium ;
- Microsoft Office 2000 Service Pack 3 ;
- Microsoft Office XP Service Pack 3.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les convertisseurs de texte WordPad et Office. Elles peuvent être exploitées à distance par le biais de documents spécialement conçus afin de faire exécuter du code arbitraire sur le système vulnérable à leur ouverture.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les convertisseurs de texte WordPad et Office. Le traitement de certains documents Word 6.0, Word97, Windows Write et WordPerfect n'est pas effectué correctement. Certains fichiers spécialement conçus peuvent ainsi corrompre la mémoire ou provoquer un dépassement de la pile.

Sous certaines conditions, l'ouverture de ces fichiers provoquera l'exécution de code arbitraire sur le système vulnérable.

L'un des correctifs empêche dorénavant WordPad d'ouvrir les fichiers Word 6.0 et Windows Write.

Certaines de ces vulnérabilités ont fait l'objet de l'alerte CERTA-2008-ALE-015 publiée le 10 décembre 2008.

5 Solution

Se référer au bulletin de sécurité MS09-010 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-010 du 14 avril 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-010.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>
- Référence CVE CVE-2008-4841 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4841>
- Référence CVE CVE-2009-0087 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0087>
- Référence CVE CVE-2009-0088 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0088>
- Référence CVE CVE-2009-0235 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0235>
- Alerte du CERTA CERTA-2008-ALE-015 publiée le 10 décembre 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-015/>

Gestion détaillée du document

15 avril 2009 version initiale.