

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans le convertisseur de fichiers Microsoft Works

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-AVI-074>

Gestion du document

Référence	CERTA-2008-AVI-074
Titre	Plusieurs vulnérabilités dans le convertisseur de fichiers Microsoft Works
Date de la première version	13 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-011 du 12 février 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

Il s'agit du convertisseur de fichiers Microsoft Works 6 inclus dans les suites :

- Microsoft Office 2003 Service Pack 2 ;
- Microsoft Office 2003 Service Pack 3 ;
- Microsoft Works 8.0 ;
- Microsoft Works Suite 2005.

3 Résumé

Trois vulnérabilités distinctes ont été identifiées dans le convertisseur de fichiers Microsoft Works 6 inclus dans certaines suites bureautiques. L'exploitation de ces dernières peut provoquer l'exécution de code arbitraire et la prise de contrôle du système vulnérable.

4 Description

Trois vulnérabilités distinctes ont été identifiées dans le convertisseur de fichiers Microsoft Works 6 inclus dans certaines suites bureautiques :

- les entrées ne seraient pas correctement manipulées, en particulier l'en-tête longueur de section présent dans les fichiers au format .wps ;
- la gestion de la table d'indexation dans l'en-tête de fichiers au format .wps ne serait pas correcte ;
- la longueur des champs dans un fichier au format .wps ne serait pas suffisamment contrôlée.

L'exploitation de ces vulnérabilités peut provoquer l'exécution de code arbitraire et la prise de contrôle du système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS08-011 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-011 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-011.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-011.msp>
- Référence CVE CVE-2007-0216 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0216>
- Référence CVE CVE-2008-0105 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0105>
- Référence CVE CVE-2008-0108 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0108>

Gestion détaillée du document

13 février 2008 version initiale.