

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans Microsoft Word

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-2006-ALE-014>

Gestion du document

Référence	CERTA-2006-ALE-014-006
Titre	Vulnérabilités dans Microsoft Word
Date de la première version	06 décembre 2006
Date de la dernière version	14 février 2007
Source(s)	Bulletin de sécurité Microsoft 929433
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 Word 2000 ;
- Microsoft Word 2002 ;
- Microsoft Word 2003 ;
- Microsoft Word Viewer 2003 ;
- Microsoft Word 2004 pour Mac ;
- Microsoft Word 2004 v. X pour Mac ;
- Microsoft Works 2004, 2005 et 2006 ;
- OpenOffice versions 2.x et antérieurs.

D'autres applications pourraient être affectées par ces vulnérabilités.

3 Résumé

Des vulnérabilités liées aux documents de format Word permettent l'exécution de code arbitraire à distance.

4 Description

4.1 Alerte du 18 décembre 2006

Trois vulnérabilités ont été découvertes dans Microsoft Word et affectent également OpenOffice. Un utilisateur malintentionné peut, en incitant sa victime à ouvrir un document au format Word (par exemple par l'intermédiaire d'un message électronique ou d'un site web), provoquer l'exécution de code arbitraire à distance avec les privilèges de l'utilisateur.

Deux codes malveillants exploitent actuellement ces vulnérabilités et sont détectés par certains antivirus (à jour) sous les noms : Troj/DwnLdr-FXG, Troj/DwnLdr-FXH, TROJ_TINY_DU, Trojan_Downloader.Win32.Cryptic.e, Trojan_Downloader.Win32.Cryptic.f, etc.

Il n'existe pas de correctif officiel pour le moment.

4.2 Mise à jour du 26 janvier 2007

Le 26 janvier 2007, Symantec fait état d'un code malveillant exploitant une nouvelle vulnérabilité non corrigée présente dans Microsoft Word 2000 (cf. section Documentation). Ce code malveillant circule sur Internet sous forme de document Word. Il est identifié par Symantec sous le nom : Trojan.Mdropper.W.

Comme les précédentes vulnérabilités, il n'existe à ce jour pas de correctif officiel.

5 Contournement provisoire

5.1 Utiliser un format de document alternatif

Le CERTA recommande l'utilisation d'un format de document alternatif tel que le RTF.

5.2 Utiliser un logiciel alternatif

Le CERTA recommande d'utiliser un outil de visualisation des documents au format Word alternatif à jour (WordPad ou AbiWord).

5.3 Mettre à jour la base de signatures d'antivirus

Certains éditeurs d'antivirus proposent déjà des mises à jours de signatures prenant en compte les codes malveillants sous sa forme actuelle. Il est cependant probable que des variantes apparaissent afin de contourner ces antivirus.

5.4 Filtrer les pièces jointes au niveau des passerelles

Dans la mesure du possible, il est recommandé de filtrer les fichiers au format Word (extension .doc) au niveau des passerelles (messagerie, web ...).

5.5 N'ouvrir que les documents provenant de sources de confiance

A la réception d'un document au format doc soit par le biais de la messagerie électronique ou sur tout autre support, il est nécessaire de s'assurer de la provenance de ce fichier et de ne l'ouvrir que si la source est de confiance et après analyse par un antivirus à jour.

5.6 Limiter l'impact en utilisant un compte utilisateur sans privilège

L'utilisation de compte n'ayant pas de droits d'administration permet de limiter l'infection au contexte de l'utilisateur.

6 Solution

Appliquer les mises à jours de l'éditeur (cf. Documentation);

7 Documentation

- Bulletins de mise à jour Microsoft MS07-014 et MS07-015 du 13 février 2007 :
<http://www.microsoft.com/technet/security/bulletin/ms07-014.msp>
<http://www.microsoft.com/technet/security/bulletin/ms07-015.msp>
- Avis du CERTA numero CERTA-2007-AVI-083 du 14 février 2007:
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-083/index.html>
- Bulletin de sécurité Microsoft 929433 du 05 décembre 2006 :
<http://www.microsoft.com/technet/security/advisory/929433.msp>
- Référence CVE CVE-2006-5994 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5994>
- Référence CVE CVE-2006-6456 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6456>
- Référence CVE CVE-2006-6561 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6561>
- Annonce sur le bloc-notes Microsoft de la seconde vulnérabilité, le 10 décembre 2006 :
<http://blogs.technet.com/msrc/archive/2006/12/10/new-report-of-a-word-zero-day.aspx>
- Annonce du bloc-note de Symantec du 26 janvier 2007 :
http://www.symantec.com/enterprise/security_response/weblog/2007/01/new_microsoft_word_2000_vulner.html
- Bulletin de sécurité Microsoft 932114 du 26 janvier 2007 :
<http://www.microsoft.com/technet/security/advisory/932114.msp>
- Référence CVE CVE-2007-0515 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0515>

Gestion détaillée du document

06 décembre 2006 version initiale.

12 décembre 2006 modifications liées à l'annonce d'une nouvelle vulnérabilité annoncée par Microsoft.

15 décembre 2006 modifications liées à l'annonce d'une nouvelle vulnérabilité, ajout des références CVE.

18 décembre 2006 modifications liées à l'affectation d'OpenOffice.

26 janvier 2007 annonce d'une nouvelle vulnérabilité par Symantec.

30 janvier 2007 ajout des références aux bulletins de sécurité Microsoft et CVE.

14 février 2007 ajout du correctif.