

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de Microsoft Windows Explorer

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-2007-ALE-007>

Gestion du document

Référence	CERTA-2007-ALE-007-001
Titre	Vulnérabilité de Microsoft Windows Explorer
Date de la première version	09 mars 2007
Date de la dernière version	09 octobre 2008
Source(s)	Alerte VU#194944 de l'US-CERT
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

Déni de service.

2 Systèmes affectés

- Microsoft Windows XP ;
- Microsoft Windows 2000.

3 Résumé

Une vulnérabilité a été découverte dans une bibliothèque de Microsoft Windows.

4 Description

Microsoft Windows Explorer utilise une bibliothèque permettant d'analyser les informations contenues dans des documents Microsoft Office.

La bibliothèque OLE32.dll serait sensible à une attaque de type *corruption de mémoire* par le biais d'un document Microsoft Office spécialement conçu.

L'exploitation de cette vulnérabilité permet au minimum de réaliser un déni de service.
Du code d'exploitation circule sur Internet.

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

L'éditeur affirme que cette vulnérabilité ne permet pas d'exécuter du code arbitraire. Cette vulnérabilité ne justifiant plus le même niveau de vigilance le CERTA a décidé de réévaluer cette alerte.

7 Documentation

- Note de vulnérabilité de l'US-CERT VU#194944 du 07 mars 2007 :
<http://www.kb.cert.org/vuls/id/194944>
- Référence CVE CVE-2007-1347 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1347>

Gestion détaillée du document

09 mars 2007 version initiale.

09 octobre 2008 réévaluation de l'alerte (passage en statut corrigé).