

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les extensions de fichiers sous Windows

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-2000-AVI-042>

Gestion du document

Référence	CERTA-2000-AVI-042
Titre	Vulnérabilité dans les extensions de fichiers sous Windows
Date de la première version	04 septembre 2000
Date de la dernière version	–
Source(s)	Security Focus
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

Contournement des protections anti virales

2 Systèmes affectés

Microsoft Office sous Windows 9x, NT 4.0 et 2000.

3 Résumé

Une personne mal intentionnée peut, en insérant des macros dans un document Office dont l'extension a été modifiée, contourner la protection de l'anti-virus.

4 Description

Sous Windows, chaque fichier porte une extension permettant l'ouverture du logiciel concerné par ce fichier (ex : .doc, .txt ...). Si une extension de fichier est inconnue de l'OS, une boîte de dialogue s'affiche afin de sélectionner une application à utiliser.

Si un fichier est créé avec Microsoft Office, mais sauvegardé avec une extension inconnue, Windows reconnaît néanmoins ce fichier et l'ouvre automatiquement avec le programme Office correspondant, Windows utilisant alors l'en-tête du fichier pour en déterminer le type.

D'autre part, la plupart des logiciels d'anti-virus, lors d'une vérification, mettent les fichiers infectés en quarantaine en modifiant leur extension. Ainsi lors de vérifications ultérieures l'anti-virus ne reconstrôle pas ce fichier.

Si un utilisateur mal intentionné crée un fichier sous Office contenant un virus macro puis l'enregistre avec l'extension d'un fichier en quarantaine, il ne sera pas vérifié lors de l'exécution de l'antivirus et sera quand même ouvert par Office..

5 Solution

– Concernant office :

Il n'existe pas de correctif pour cette vulnérabilité, cependant lorsqu'il est bien configuré, Word ouvre une boîte de dialogue proposant à l'utilisateur le choix d'exécuter ou non les macros. Il est nécessaire d'activer ce type d'alerte.

Sous Word :

- Menu : Outil
- Choix : Option
- Onglet : Général
- Sélectionner : Protection contre les virus contenus dans les macros.

En résumé, si le lancement d'un fichier ayant une extension inconnue ouvre Office et présente la boîte de dialogue concernant les macros, il est impératif de sélectionner « Ne pas ouvrir » afin d'éviter l'exécution de la macro.

– Concernant l'anti-virus :

Par défaut, les anti-virus sont paramétrés afin de ne pas scanner différents types d'extension de fichiers. Il est recommandé de supprimer ces types d'extension de la liste d'exclusion de votre anti-virus.

6 Documentation

Aucune documentation actuellement disponible.

Gestion détaillée du document

04 septembre 2000 version initiale.