

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la fonction de « fusion-publipostage » sous Word 97 et 2000

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-056>

Gestion du document

Référence	CERTA-2000-AVI-056
Titre	Vulnérabilité dans la fonction de « fusion-publipostage » sous Word 97 et 2000
Date de la première version	09 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Microsoft
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.

2 Systèmes affectés

Les logiciels touchés sont Microsoft Word 97 et 2000. La vulnérabilité est indépendante de la plate-forme.

3 Résumé

Une vulnérabilité de la fonction « fusion-publipostage » de WORD 97 et 2000 permet l'exécution de code écrit en Visual Basic (VBA) à l'insu de l'utilisateur de WORD.

4 Description

La fonction de « fusion-publipostage » est une fonction de WORD permettant la création de multiples documents à partir d'un modèle de document unique et d'une source extérieure (base de données, tableau, etc.) afin de diffuser des documents à des listes de destinataires, de créer des étiquettes ou des catalogues, etc.

Lorsqu'un utilisateur ouvre un document contenant un appel de la fonction « fusion-publipostage » dont la source extérieure contient notamment du code VBA situé dans une base de donnée (Access), celui-ci sera exécuté à l'insu de l'utilisateur.

Pour que cette exploitation de la vulnérabilité soit réalisable, il faut que l'accès à la base de donnée malicieuse soit fait au travers d'un chemin UNC ou d'un lien de type `file:///`.

5 Solution

Pour Word 2000 Appliquer le correctif de Microsoft :

<http://officeupdate.microsoft.com/2000/DownloadDetails/wrdacc.htm>

Le correctif pour Word 97 n'est pas disponible. Consultez régulièrement le site pour savoir s'il y a du nouveau.

6 Documentation

– Le bulletin de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms00-071.asp>

– La FAQ sur le bulletin de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/fq00-071.asp>

Gestion détaillée du document

09 octobre 2000 version initiale.