Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 22 mai 2001
N° CERTA-2001-AVI-056

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Word lors de l'ouverture de documents RTF

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-2001-AVI-056

Gestion du document

Référence	CERTA-2001-AVI-056
Titre	Vulnérabilité dans Word lors de l'ouverture de documents RTF
Date de la première version	22 mai 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-028
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 macros sans fenêtre d'avertissement.

2 Systèmes affectés

- Microsoft Word 97 ;
- Microsoft Word 2000 ;
- Microsoft Word 98 ;
- Microsoft Word 98 pour Mac ;
- Microsoft Word 2001 pour Mac.

3 Résumé

Une macro insérée dans un modèle de document RTF peut être exécutée par Word sans affichage d'une fenêtre avertissant la présence de cette macro.

4 Description

Théoriquement, lors de l'ouverture d'un document contenant une macro, Word propose à l'utilisateur le choix d'ouvrir le document en prenant en compte ou non cette macro.

Le format RTF (Format de texte enrichi) est couramment utilisé car il est reconnu par la plupart des logiciels de traitement de texte. Par ailleurs il est réputé plus sur que les documents au format DOC car il n'est pas censé contenir de macro.

Les modèles types de document sont utilisés par exemple pour prévoir des en-têtes et des pieds de page. Ils peuvent être utilisés en relation avec tout document texte.

Une vulnérabilité de Word permet, si un fichier RTF est associé à un modèle type contenant une macro, d'exécuter cette macro sans demande préalable. Car Word ne vérifie lors de l'ouverture que la constitution du document RTF.

Cette macro peut être par exemple un virus et peut exécuter n'importe quelle tâche sur la machine cible avec les privilèges de l'utilisateur.

5 Solution

Télécharger le correctif sur le site Web Microsoft :

- Correctif pour Microsoft Word 2000 :
  http://office.microsoft.com/downloads/2000/wd2kmsec.aspx
- Correctif pour Microsoft Word 97 :
  http://office.microsoft.com/downloads/9798/wd97mcrs.aspx
- Concernant Word 98, 98 et 2001 pour Mac les correctifs ne sont actuellement pas disponibles.

6 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-028.asp

Gestion détaillée du document

22 mai 2001 version initiale.