

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité sous Windows liée à l'ouverture d'un Document Office

---

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-052>

---

### Gestion du document

Référence	CERTA-2000-AVI-052
Titre	Vulnérabilité sous Windows liée à l'ouverture d'un Document Office
Date de la première version	25 septembre 2000
Date de la dernière version	–
Source(s)	Georgi Guninski SecurityFocus et BugTraq
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

Tout les systèmes Microsoft Windows, avec des applications Office telles que Word ou Excel dans le cas présent.

## 3 Résumé

Si une librairie dynamique particulière se situe dans le même répertoire qu'un document Office quelconque, elle sera exécutée à condition que l'ouverture de ce document via l'explorateur lance l'application associée.

## 4 Description

Lors de l'ouverture d'un fichier par une application Office, si le système a besoin d'une librairie dynamique, il la recherche d'abord dans le répertoire de l'application, le répertoire où se trouve le fichier ouvert, puis dans

les répertoires systèmes de Windows et enfin dans les répertoires indiqués par les chemins listés dans la variable PATH.

Les bibliothèques msi.dll et Riched20.dll, sont normalement situées dans le répertoire winnt/system32 de Windows NT, et Windows/system dans le cas de windows 9x, et sont utilisées lors de l'exécution de WORD ou d'EXCEL (seulement msi.dll dans ce dernier cas).

Un utilisateur mal intentionné peut s'arranger pour qu'une de ces bibliothèques, qu'il aura modifiée au préalable en y mettant du code malicieux, soit située dans le même répertoire qu'un document que sa victime aura à ouvrir. Si l'application office n'est pas déjà ouverte, la bibliothèque falsifiée sera chargée et exécutée.

## 5 Contournement provisoire

Le fait que l'application Office soit déjà ouverte empêche ce phénomène, car la bibliothèque à charger en mémoire est déjà ouverte depuis le chemin nominal.

Il ne faut donc jamais ouvrir un document par un double-clic, ni par le menu contextuel de l'explorateur, mais exécuter l'application qui y est associée, et ouvrir le document à partir du menu fichier de l'application.

Désactiver, dans l'explorateur, l'association des fichiers .doc et .dot avec WORD et .xls avec EXCEL.

Dans le menu *affichage* de l'explorateur ou du poste de travail, choisir *options*, dans la fenêtre qui s'ouvre, sélectionner l'onglet *types de fichiers*, enfin supprimer les entrées pour les types de documents indiqués.

Vérifier qu'il n'y a pas de fichiers bibliothèques .DLL dans des répertoires ne contenant que des données. Elle ne devraient pas y être.

## 6 Documentation

Aucune documentation additionnelle.

## Gestion détaillée du document

25 septembre 2000 version initiale.