Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 juin 2002
N° CERTA-2002-AVI-132

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Excel et Word pour Windows

Gestion du document

Référence	CERTA-2002-AVI-132
Titre	Multiples vulnérabilités dans Excel et Word pour Windows
Date de la première version	21 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS02-031 de 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 ;
- risque de propagation de virus.

2 Systèmes affectés

- Microsoft Excel 2000 pour Windows ;
- Microsoft Office 2000 pour Windows ;
- Microsoft Excel 2002 pour Windows ;
- Microsoft Word 2002 pour Windows ;
- Microsoft Office XP pour Windows.

3 Résumé

Un utilisateur mal intentionné peut composer un document Excel ou Word contenant des macros spécifiques permettant d'exécuter du code arbitraire sur la machine cible.

4 Description

Un module spécifique permet d'informer l'utilisateur de la présence d'une ou plusieurs macros lors de l'ouverture d'un document Excel ou Word. Un utilisateur mal intentionné peut, par le biais d'un document judicieusement composé, contourner ce module et exécuter des macros à l'insu de l'utilisateur.

Microsoft a créé le système DDE (Dynamic Data Exchange) pour pouvoir utiliser des données partagées entre plusieurs applications. Normalement, chaque application vérifie et informe l'utilisateur si une macro doit être exécutée. Mais il arrive qu'une macro soit exécutée dans un objet importé grâce à DDE sans que l'utilisateur n'en soit averti.

Quatre nouvelles vulnérabilités de ce type ont été découvertes :

- Si un objet contenant une macro est importé dans une feuille de calcul Excel, le fait de cliquer sur cet objet exécute la macro sans que l'utilisateur n'en soit averti ;
- si un dessin est pourvu d'un lien pointant sur une feuille de calcul Excel, une macro contenue dans cette feuille de calcul est exécutée sans que l'utilisateur n'en soit averti ;
- si une feuille de calcul Excel au format XSL contient du script HTML, ce script est exécuté sans en avertir l'utilisateur ;
- Word peut utiliser Access pour en extraire des données. Si la base Access contient une macro, celle-ci est exécutée sans en avertir l'utilisateur.

Ce type de vulnérabilité peut servir à exécuter du code arbitraire, comme par exemple des virus ou des chevaux de Troie.

5 Solution

Des correctifs sont disponibles en téléchargement sur le site web de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS02-031.asp

6 Documentation

Bulletin de sécurité #MS02-031 de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS02-031.asp

Gestion détaillée du document

21 juin 2002 version initiale.