Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 septembre 2003
N° CERTA-2003-AVI-147

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Visual Basic pour Applications (VBA)

Gestion du document

Référence	CERTA-2003-AVI-147
Titre	Vulnérabilité dans Visual Basic pour Applications (VBA)
Date de la première version	04 septembre 2003
Date de la dernière version	–
Source(s)	Avis MS03-037 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.

2 Systèmes affectés

Microsoft Visual Basic pour Applications SDK 5.0, 6.0, 6.2 et 6.3.
Ces versions de Visual Basic pour Applications sont incluses dans les produits suivants :

- Microsoft Access 97, 2000 et 2002 ;
- Microsoft Excel 97, 2000 et 2002 ;
- Microsoft PowerPoint 97, 2000 et 2002 ;
- Microsoft Project 2000 et 2002 ;
- Microsoft Publisher 2002 ;
- Microsoft Visio 2000 et 2002 ;
- Microsoft Word 97, 98(J), 2000 et 2002 ;
- Microsoft Works Suite 2001, 2002 et 2003 ;
- Microsoft Business Solutions Great Plains 7.5 ;
- Microsoft Business Solutions Dynamics 6.0 et 7.0 ;
- Microsoft Business Solutions eEnterprise 6.0 et 7.0 ;
- Microsoft Business Solutions Solomon 4.5, 5.0 et 5.5.

3 Résumé

Une vulnérabilité dans Visual Basic pour Applications (VBA) permet l'exécution de code arbitraire.

4 Description

Microsoft Visual Basic pour Applications (VBA) est un outil de développement qui permet de personnaliser des progiciels et de les intégrer à des données et à des systèmes existants.

Les produits de la suite Microsoft Office font appel à VBA pour exécuter certaines fonctions.

Une vulnérabilité dans la vérification des propriétés d'un document lors de son ouverture par VBA permet l'exécution de code arbitraire sur la machine. Les documents habilement construits permettant l'exploitation de la vulnérabilité sont ceux reconnus par un produit incluant VBA (documents Word, Excel, Access...). Dans le cas où Microsoft Word est utilisé comme éditeur HTML par Microsoft Outlook, le document est alors un mèl, et la vulnérabilité ne peut être exploitée que si un utilisateur répond ou transfère ce message.

5 Solution

Installer le correctif indiqué à l'adresse suivante :
http://www.microsoft.com/technet/security/bulletin/ms03-037.asp

6 Documentation

http://www.microsoft.com/technet/security/bulletin/ms03-037.asp

Gestion détaillée du document

04 septembre 2003 version initiale.