Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 août 2000
N° CERTA-2000-AVI-027

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans les documents HTML d'Office 2000

Gestion du document

Référence	CERTA-2000-AVI-027
Titre	Débordement de mémoire dans les documents HTML d'Office 2000
Date de la première version	16 août 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

Débordement de mémoire permettant l'execution de code arbitraire, l'usurpation des droits de l'utilisateur courant, ou causant un bloquage de la machine.

2 Systèmes affectés

Indépendemant du système d'exploitation :
- WORD 2000
- EXCEL 2000
- POWERPOINT 2000

3 Résumé

Une erreur dans la gestion de la conversion des documents HTML a été découverte dans la conception des outils de la suite Office. Une page HTML habilement conçue permet de bloquer la machine voire de lui faire exécuter du code arbitraire.

Nota : Les logiciels cités, même installés séparéments, sont vulnérables.

4 Description

Un utilisateur malintentionné peut créer une page HTML contenant une balise « Object » malformée. Ce document enregistré, au préalable comme un « Document Office » , bloquera le logiciel (précédement listé) qui l'ouvrira.

Pour faire ouvrir le document par sa victime, l'utilisateur malicieux pourra présenter le document comme un fichier attaché à un courrier électronique, ou un fichier à télecharger sur un site web, ou le transmettre par tout autre média : disquette, CD-ROM, etc...

5 Contournement provisoire

Sous WORD 2000 uniquement, il est possible d'empêcher ce débordement de mémoire par le moyen suivant :

Dans le menu Outils, rubrique Options, onglet Général : désactiver l'option « Confirmation des conversions lors de l'ouverture »

Suivre les recommandations faites précédement concernant les documents attachés ou télechargés.

6 Solution

Microsoft a mis au point un correctif disponible à l'adresse suivante :
http://officeupdate.microsoft.com/2000/downloadDetails/Of9data.htm
`Nota` : Ce correctif doit être appliqué après Office 2000 SR-1 (Service Release 1).
Correctif testé sur la version française d'Office 2000.

7 Documentation

- Le bulletin de Sécurité de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms00-056.asp
- La FAQ de ce bulletin :
  http://www.microsoft.com/technet/security/bulletin/fq00-056.asp
- L'article de la base de connaissances de Microsoft :
  http://www.microsoft.com/technet/support/kb.asp?ID=269880

Gestion détaillée du document

16 août 2000 version initiale.