

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Internet Explorer 4.01, Office 2000 et PowerPoint 97

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-016>

Gestion du document

Référence	CERTA-2000-AVI-016
Titre	Vulnérabilités dans Internet Explorer 4.01, Office 2000 et PowerPoint 97
Date de la première version	19 juillet 2000
Date de la dernière version	–
Source(s)	Microsoft Security Bulletin Avis du CERT IST
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 ;
- Téléchargement de fichiers sur le système.

Des exemples d'utilisation de cette vulnérabilité sont facilement disponibles.

2 Systèmes affectés

- Internet Explorer 4.01 SP 2 et supérieur ;
- Microsoft Office 2000 ;
- PowerPoint 97.

3 Résumé

Deux vulnérabilités ont été découvertes, l'une permettant sous Internet Explorer 4.01 SP 2 d'exécuter une macro VBA, l'autre sous Office 2000 et PowerPoint 97 permettant de sauvegarder un fichier sur le disque à l'insu de son utilisateur.

4 Description

- Première vulnérabilité (Internet Explorer 4.01 SP 2) :

Un site malveillant peut proposer un script qui ouvre une base de données Access (Type MDB) disponible sur ce site. Le fichier MDB pourrait contenir des macros qui s'exécuteraient sans prévenir l'utilisateur.

Sous Outlook et Outlook Express, le fait d'afficher un mël au format HTML peut conduire au même résultat.

- Deuxième vulnérabilité (Office 2000 et PowerPoint 97) :

Un site malveillant peut proposer un script qui permet de faire appel à un objet Excel ou PowerPoint situé sur la machine de l'utilisateur afin qu'un fichier, se trouvant sur le site, soit sauvegardé sur la machine locale.

5 Contournement provisoire

Première vulnérabilité (Internet Explorer 4.01 SP 2) :

Aucun correctif n'est disponible actuellement auprès de Microsoft, cependant un contournement du problème peut être réalisé en définissant un mot de passe pour l'administrateur Access. Cette solution permet une invite de saisie du mot de passe avant l'exécution d'un script VBA.

Mise en place du mot de passe :

- Démarrer Acces 2000 sans ouvrir de base de données
- Menu « outils », Choix « sécurisé », « Définition des utilisateurs de groupes »
- Sélectionner « administrateur » en utilisateur courant
- Sélectionner l'onglet « Changer le mot de passe »
- Laisser l'ancien mot de passe vide puis saisir le nouveau

6 Solution

Deuxième vulnérabilité (Office 2000 et PowerPoint 97) :

Correctif pour Office 2000 et PowerPoint 2000 :

<http://officeupdate.microsoft.com/2000/downloaddetails/Addinsec.htm>

Correctif pour PowerPoint 97 :

<http://officeupdate.microsoft.com/downloaddetails/PPT97sec.htm>

7 Documentation

Bulletin Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms00-049.asp>

Gestion détaillée du document

19 juillet 2000 version initiale.