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 juillet 2002
N° CERTA-2001-AVI-041-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Internet Explorer 5.01 et 5.5

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-2001-AVI-041

Gestion du document

Référence	CERTA-2001-AVI-041-001
Titre	Vulnérabilité dans Internet Explorer 5.01 et 5.5
Date de la première version	30 mars 2001
Date de la dernière version	16 juillet 2002
Source(s)	Bulletin de sécurité Microsoft (MS01-020)
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 ;
- propagation de ver et de virus.

2 Systèmes affectés

- Microsoft Internet Explorer versions 5.01 et 5.5.

3 Résumé

Un utilisateur mal intentionné peut envoyer par mél ou disposer sur un site web une page HTML habilement conçue dans le but d'exécuter du code arbitraire sur la machine cible.

4 Description

Outlook et Outlook express utilisent des composants d'Internet Explorer afin d'assurer la lecture des méls au format HTML. Internet Explorer détermine en fonction du type MIME du fichier l'application à activer pour en assurer la lecture (exemple : fichier texte, vidéo, audio, etc...).

Une vulnérabilité d'Internet Explorer dans l'interprétation de l'entête MIME permet à un utilisateur mal intentionnéd'exécuter du code arbitraire avec les privilèges du destinataire du message.

Sous Outlook, il existe un « volet de prévisualisation » qui permet de voir le message dès qu'il est sélectionné. Il est activé par défaut dans la configuration d'outlook.

Il est également possible d'insérer ce type de code dans une page HTML habilement conçue afin de le faire exécuter par le navigateur.

5 Contournement provisoire

Dans l'impossibilité d'appliquer le correctif immédiatement (absence de la personne ayant les permissions adéquates sur la système par exemple), utiliser le moyen temporaire suivant :

Il est possible de bloquer le téléchargement automatique de fichiers dans les paramètres d'Internet Explorer :

- Menu : Outils ;
- sélectoionner : Options Internet ;
- onglet : sécurité ;
- choix : Personnaliser le niveau ;
- désactiver : Téléchargement de fichiers.

6 Solution

- Appliquer le correctif de Microsoft :
  http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp
- Le Service Pack 2 d'Internet Explorer 5.5 ou 5.01 corrige cette vulnérabilité entre-autres :
  http:///www.microsoft.com/windows/ie/downloads/archive/default.asp
- Installer Internet Explorer 6 :
  http://www.microsoft.com/windows/ie/downloads/ie6/default.asp

`Nota` : Pour prendre connaissance de la version d'Internet Explorer et des correctif ou *Service Packs* qui y ont été appliqués, procédez comme suit :

1. Démarrer le navigateur Internet Explorer ;
2. menu : «?» (A propos) ;
3. sélectionner : A propos d'Internet Explorer ;
4. le champ : `Versions des mises à jour` (ou *Updates Versions* permet de connaitre les correctifs et *Service Packs* qui ont été appliqués.
   La figure 1 montre une version d'Internet Explorer 5.01 sans aucun correctif appliqué. La figure 2 montre une version de Internet Explorer 5.5 corrigée avec le Service Pack 2 (indiqué par : `;SP2;`)

`Attention` :le champ nommé « version: » indique la version du navigateur. Mais pour la version `5.01` d'internet explorer, ce champ commencera par `5.00`. Les huits autres chiffres correspondent au correctifs appliqués ainsi qu'aux *Service Packs*.

7 Documentation

Bulletin de sécurité MS01-020 de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

Gestion détaillée du document

30 mars 2001 version initiale.

16 juillet 2002 seconde version : propagation intensive des vers utilisant cette vulnérabilité.

FIG. 1 – *Internet Explorer 5.01 non corrigé*

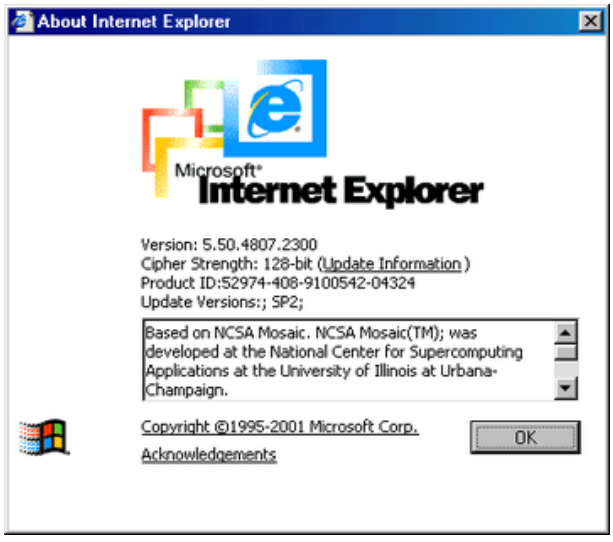

FIG. 2 – *Internet Explorer 5.5 corrigé*