Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 décembre 2000
N° CERTA-2000-AVI-082

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sous Microsoft Internet Explorer 5.x

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-082

Gestion du document

Référence	CERTA-2000-AVI-082
Titre	Vulnérabilités sous Microsoft Internet Explorer 5.x
Date de la première version	05 décembre 2000
Date de la dernière version	–
Source(s)	Bulletin Microsoft (MS00-093)
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 ;
- Compromission des données.

2 Systèmes affectés

Microsoft Internet Explorer 5.x

3 Résumé

Plusieurs vulnérablités sous Microsoft Internet Explorer version 5.x permettent à un administrateur d'un site internet de pouvoir lire des fichiers se trouvant sur la machine distante ou d'exécuter du code.

4 Description

4.1 Première vulnérabilité - Uniquement IE 5.5

Une fonctionnalité d'IE 5.5 permet de formater une page internet en vue de son impression. Une vulnérabilité permet à un concepteur de site mal intentionné, par le biais de contrôles ActiveX, d'exécuter du code ou d'avoir

un accès total sur les fichiers de la machine vulnérable.

4.2 Deuxième vulnérabilité

Parmi les différentes méthodes permettant de remplir un formulaire Web, l'une d'elle permet de saisir un nom de fichier à télécharger sur le site distant. Cette vulnérabilité permet à un site maliceux de lire des fichiers sur la machine de l'utilisateur.

4.3 Troisième vulnérabilité

Une variante de la vulnérabilité MS00-055, permet à un concepteur malicieux de site internet d'avoir accès aux fichiers du poste utilisateur par le biais de scripts habilement construits.

4.4 Quatrième vulnérabilité

Une variante des vulnérabilités MS00-0033 et MS00-0055 permet à un concepteur de site de modifier l'exécution des «frames» afin d'afficher dans la première fenêtre son domaine et dans la seconde le contenu du système de fichiers de l'utilisateur local.

5 Solution

Appliquer le correctif Microsoft :
http://www.microsoft.com/windows/ie/download/critical/279328

6 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS00-093.asp

FAQ Microsoft :
http://www.microsoft.com/technet/security/bulletin/fq00-093.asp

Gestion détaillée du document

05 décembre 2000 version initiale.