



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 février 2002
N° CERTA-2002-AVI-030-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'Internet Explorer

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-2002-AVI-030>

Gestion du document

Référence	CERTA-2002-AVI-030-001
Titre	Multiples vulnérabilités d'Internet Explorer
Date de la première version	12 février 2002
Date de la dernière version	21 février 2002
Source(s)	Bulletin de sécurité Microsoft MS02-005
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 ;
- contournement des règles de sécurité ;
- accès non-autorisé aux données.

2 Systèmes affectés

Tout système d'exploitation Windows muni du navigateur Internet Explorer version 5.01, 5.5 ou 6.

3 Résumé

Six vulnérabilités différentes ont été découvertes sur les navigateurs Internet Explorer 5.01, 5.5 et 6.

4 Description

- Un utilisateur mal intentionné peut, en créant une page web invoquant des directives HTML permettant d'incorporer un document dans une page web, effectuer un débordement de mémoire du navigateur de l'internaute qui lit cette page. Ce débordement de mémoire permet d'exécuter du code arbitraire sur le système de la victime.
- La fonction `GetObject` effectue des tests de sécurité lors d'une requête vers un objet du système. Une vulnérabilité de cette fonction permet d'éviter ces tests de sécurité préalables en utilisant une représentation habilement conçue du chemin d'un fichier. Il est notamment possible d'accéder à des fichiers non autorisés sur la machine victime par le biais d'une opération incluse dans une page web astucieusement construite.
- Un mauvais fonctionnement de l'affichage des noms de fichiers à télécharger par le navigateur permet à un utilisateur mal intentionné de tromper la vigilance de sa victime en modifiant l'affichage du nom (type) de fichier à télécharger au moyen des champs des entêtes MIME.
- Une vulnérabilité de la gestion des applications listées dans Internet Explorer permet d'ouvrir un document situé sur un site au moyen d'une application ne correspondant pas à celle préconisée pour ce type de document. De plus, une application n'apparaissant pas dans la liste des applications sûres d'Internet Explorer peut aussi être utilisée pour l'ouverture de ce document.
- Une vulnérabilité du navigateur permet d'exécuter des scripts même si ce paramètre a été désactivé. En effet la vérification de la présence de scripts se fait avant l'affichage de la page. Or il existe un moyen d'incorporer des objets qui répondent à des événements asynchrones ce qui permet l'exécution de scripts contenus dans ces objets après la vérification préalable de l'absence de scripts.
- Une variante de la vulnérabilité décrite dans le bulletin MS01-058 (CERTA-2001-AVI-163) permet à un administrateur de site web mal intentionné de faire ouvrir deux fenêtres par le navigateur de sa victime et de lire au travers de l'une d'entre elles n'importe quel fichier présent sur la machine de la victime par le biais de la fonction `Document.Open` par exemple.

5 Contournement provisoire

- Pour que certaines de ces vulnérabilités ne soient pas exploitables trop simplement (utilisation de `GetObject` ou `Document.Open`), désactiver les scripts (Java, JavaScripts et ActiveX).
- Concernant le téléchargement d'un fichier, il ne faut jamais l'ouvrir directement sans le sauvegarder. Après sa sauvegarde et avant son ouverture, il est recommandé de l'analyser avec un antivirus à jour. Enfin, il est déconseillé de double-cliquer sur un fichier. Il vaut mieux choisir judicieusement l'application qui permet de le visualiser et l'ouvrir par le menu `fichier/ouvrir` de cette dernière.
- En attendant de télécharger le correctif, utiliser temporairement un autre navigateur web.

6 Solution

Appliquer le correctif cumulatif de Microsoft :

<http://www.microsoft.com/windows/ie/downloads/critical/q316059/default.asp>

7 Documentation

<http://www.microsoft.com/technet/security/bulletin/MS02-005.ASP>

Gestion détaillée du document

12 février 2002 version initiale.

21 février 2002 seconde version : erreur dans l'URL du correctif (paragraphe Solution)