



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 03 août 2004  
N° CERTA-2004-ALE-009-003

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : 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-2004-ALE-009>

---

### Gestion du document

Référence	CERTA-2004-ALE-009-003
Titre	Vulnérabilités d'Internet Explorer
Date de la première version	09 juin 2004
Date de la dernière version	03 août 2004
Source(s)	Liste de discussion Full-Disclosure
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

- Accès aux ressources locales ;
- contournement de la politique de sécurité ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Microsoft Internet Explorer 6.

La vulnérabilité du composant ADODB.Stream affecte également les versions 5.x d'Internet Explorer.

## 3 Résumé

Plusieurs vulnérabilités d'Internet Explorer version 6 non corrigées à ce jour permettent à un utilisateur mal intentionné d'accéder aux ressources locales de la machine, de contourner la politique de sécurité et d'exécuter du code arbitraire à distance.

## 4 Description

Deux vulnérabilités ont été découvertes dans le navigateur Internet Explorer version 6 :

- la première vulnérabilité concerne les fichiers d'aide de type CHM au format Microsoft ITS et permet d'accéder aux ressources locales de la machine cible. Cet accès s'effectue par le biais du champ *Location* de l'en-tête HTTP.
- La deuxième vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code avec les privilèges de la zone *Machine locale*.

Cette deuxième vulnérabilité permet d'exploiter une autre faille de sécurité : celle de l'activeX *ADODB.Stream*. Cette vulnérabilité est connue depuis longtemps mais avait été jugée par Microsoft comme "non dangereuse", puisqu'il était nécessaire de contourner le mécanisme des zones de sécurité pour l'exploiter.

Ces vulnérabilités sont actuellement exploitées via un document au format HTML ou un site web malicieusement construit, pour exécuter du code arbitraire sur un système vulnérable.

## 5 Contournement provisoire

- Désactiver l'exécution de scripts pour tous les sites web qui ne sont pas de confiance ;
- désactiver la gestion du protocole ITS. Pour cela, renommer les clefs du registre Microsoft suivantes :  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler\ms-its  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler\its  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler\mk  
Note : on pourra renommer ces clefs de registre en ajoutant -off (ms-its devient ms-its-off)
- désactiver le composant *ADODB.Stream* d'Internet Explorer (cf. section Documentation).

## 6 Solution

Se référer au bulletin de sécurité MS04-025 de Microsoft afin d'obtenir la liste des correctifs (cf. Documentation).

## 7 Documentation

- Message de la liste de discussion Full-Disclosure :  
<http://archives.neohapsis.com/archives/fulldisclosure/2004-06/0104.html>
- Avis de sécurité Secunia SA11793 du 08 juin 2004 :  
<http://secunia.com/advisories/11793/>
- Fiche technique de Microsoft pour désinstaller le composant *ADODB.Stream*  
<http://support.microsoft.com/?kbid=870669>
- Bulletin de sécurité Microsoft MS04-025 du 01 Août 2004 :  
<http://www.microsoft.com/technet/security/bulletin/ms04-025.msp>
- Avis CERTA-2004-AVI-260 du CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-260/>

## Gestion détaillée du document

**09 juin 2004** version initiale.

**02 juillet 2004** première révision : prise en compte de la vulnérabilité *ADODB.Stream* et ajout du lien pour la désinstallation du composant.

**05 juillet 2004** deuxième révision : modification des versions affectées et prise en compte de l'exploitation des vulnérabilités.

**03 août 2004** troisième révision : ajout de la section solution et des références des avis de Microsoft et du CERTA.