



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 octobre 2003  
N° CERTA-2003-ALE-004-001

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité 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-2003-ALE-004>

---

### Gestion du document

Référence	CERTA-2003-ALE-004-001
Titre	Vulnérabilité d'Internet Explorer
Date de la première version	10 septembre 2003
Date de la dernière version	06 octobre 2003
Source(s)	Bulletin de sécurité MS03-032 de Microsoft Note VU#865940 du CERT/CC
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 à distance.

## 2 Systèmes affectés

- Microsoft Internet Explorer versions 5.01, 5.5 et 6.0 ;
- Microsoft Internet Explorer version 6.0 pour Windows Server 2003.

## 3 Description

Dans le bulletin de sécurité MS03-032 "Cumulative Patch for Internet Explorer" (se référer au bulletin CERTA-2003-AVI-139), Microsoft annonçait publiquement l'existence d'une vulnérabilité liée à un contrôle incorrect du type de données spécifié dans l'attribut data de la balise object et publiait un correctif.

Cette vulnérabilité peut être exploitée au moyen d'un site web ou d'un message électronique au format HTML habilement constitué et permettre ainsi à un utilisateur mal intentionné d'exécuter du code arbitraire sur la plateforme vulnérable.

Depuis la sortie du bulletin, il a été démontré que le correctif proposé par Microsoft ne prévient pas l'exploitation de la vulnérabilité dans le cas où le document appelant n'est pas un document HTML statique.

Des techniques d'exploitation de cette vulnérabilité à partir de documents HTML générés dynamiquement ont largement été décrites dans plusieurs forums sur l'Internet.

## 4 Contournement provisoire

Dans l'attente de l'application du correctif, il est fortement conseillé de prendre certaines précautions :

- limiter la consultation des sites WEB, respecter les règles d'usage relatives à la messagerie (se référer à la note d'information CERTA-2000-INF-002) ;
- désactiver le support des contrôles Active X au niveau d'Internet Explorer ;
- renommer ou supprimer la clef de registre  
HKLM\SOFTWARE\Classes\MIME\Database\Content Type\application/hta empêchant ainsi l'exécution de documents au format application/hta.

## 5 Solution

La version 1.4 du bulletin de sécurité MS03-032 "Cumulative Patch for Internet Explorer" mentionne l'existence d'un nouveau bulletin de sécurité MS03-040 "Cumulative Patch for Internet Explorer".

Se référer au bulletin de sécurité MS03-040 (cf. section Documentation) pour la disponibilité du correctif.

## 6 Documentation

- Bulletin de sécurité MS03-032 "Cumulative Patch for Internet Explorer" :  
<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>
- Bulletin de sécurité MS03-040 "Cumulative Patch for Internet Explorer" :  
<http://www.microsoft.com/technet/security/bulletin/MS03-040.asp>
- Bulletin CERTA-2003-AVI-139 "Multiples vulnérabilités dans Internet Explorer" :  
<http://www.certa.ssi.gouv.fr>
- Note d'information CERTA-2000-INF-002 "Mesures de préventions relatives à la messagerie" :  
<http://www.certa.ssi.gouv.fr>
- Note VU#865940 du cert/cc :  
<http://www.kb.cert.org/vuls/id/865940>

## Gestion détaillée du document

**10 septembre 2003** version initiale.

**06 octobre 2003** Ajout d'une section Solution référençant le correctif Microsoft.