



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 29 mars 2002  
N° CERTA-2002-AVI-066

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans 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-066>

---

### Gestion du document

Référence	CERTA-2002-AVI-066
Titre	Vulnérabilités dans Internet Explorer
Date de la première version	29 mars 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-015
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 ;
- Atténuation des paramètres de sécurité.

## 2 Systèmes affectés

- Microsoft Internet Explorer 5.01 ;
- Microsoft Internet Explorer 5.5 ;
- Microsoft Internet Explorer 6.0.

## 3 Résumé

Deux vulnérabilités ont été découvertes dans Internet Explorer.

La première vulnérabilité permet, par le biais d'un cookie judicieusement composé, de changer la détermination de zone d'Internet Explorer diminuant ainsi les restrictions.

La seconde vulnérabilité permet, lors de la visite d'une page web habilement conçue, d'exécuter n'importe quel programme présent sur la machine cible.

## 4 Description

– Première vulnérabilité :

Sur Internet Explorer une notion de zone permet d'accorder différents niveaux de confiance aux sites visités. Suivant ces niveaux, plusieurs restrictions sont effectuées pour l'exécution de code ou autre. Par principe, les sites Internet distants sont considérés dans la Zone Internet. Un concepteur de site mal intentionné peut créer un cookie composé de code HTML qui sera déposé, lors de la visite sur le site, dans la machine cible.

Quand ce cookie sera à nouveau consulté, le code qu'il contient sera automatiquement exécuté en Zone Locale et non Zone Internet diminuant ainsi les restrictions.

– Seconde vulnérabilité :

L'objet `CodeBase` permet de définir l'emplacement où un fichier, récupéré par le biais d'une page Web, va être enregistré.

Une vulnérabilité présente dans cet objet permet d'exécuter n'importe quel programme présent sur une machine.

Un concepteur de site mal intentionné ayant réalisé une page web exploitant cette vulnérabilité pourrait faire exécuter n'importe quel programme sur la machine cible. Cependant aucun paramètre ne peut être ajouté à la commande.

## 5 Contournement provisoire

Concernant la première vulnérabilité, il est conseillé de désactiver les cookies.

## 6 Solution

Télécharger le correctif sur le site Microsoft :

<http://www.microsoft.com/windows/ie/downloads/critical/Q319182/default.asp>

## 7 Documentation

Bulletin Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS02-015.asp>

## Gestion détaillée du document

29 mars 2002 version initiale.