



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 02 décembre 2004  
N° CERTA-2004-AVI-383

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Internet Explorer 6

---

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-AVI-383>

---

### Gestion du document

Référence	CERTA-2004-AVI-383
Titre	Vulnérabilité dans Internet Explorer 6
Date de la première version	02 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-040 Bulletin d'alerte de sécurité CERTA-2004-ALE-012
Pièce(s) jointe(s)	

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

- Internet Explorer 6 Service Pack 1 sous Microsoft Windows 2000 Service Pack 3 & Service Pack 4 ;
- Internet Explorer 6 Service Pack 1 sous Microsoft Windows XP Service Pack 1 ;
- Internet Explorer 6 Service Pack 1 sous Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Internet Explorer 6 Service Pack 1 sous Microsoft Windows NT Server 4.0 Terminal Service Edition Service Pack 6 ;
- Internet Explorer 6 Service Pack 1 sous Microsoft Windows 98, Windows 98 SE & Windows Me ;
- Internet Explorer 6 sous Microsoft Windows XP Service Pack 1 (64-bit Edition).

## 3 Résumé

Une vulnérabilité découverte dans Internet Explorer 6 permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

## **4 Description**

Le logiciel de navigation Internet Explorer 6 de Microsoft présente une vulnérabilité de type débordement de mémoire (Buffer Overflow) due à un mauvais traitement des attributs SRC et NAME des balises <FRAME>et <IFRAME>qui permettent aux développeurs d'insérer des cadres dans une page HTML. Cette vulnérabilité permet à une personne mal intentionnée d'exécuter du code arbitraire, avec les privilèges de la victime, à l'aide d'une page HTML ou d'un courrier électronique malicieusement constitué.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

## **6 Documentation**

- Bulletin de sécurité Microsoft MS04-040 :  
<http://www.microsoft.com/technet/security/bulletin/MS04-040.mspx>
- Bulletin d'alerte CERTA-2004-ALE-012 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-012/index.html>

## **Gestion détaillée du document**

**02 décembre 2004** version initiale.