

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Internet Explorer sous Mac OS

---

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-081>

---

### Gestion du document

Référence	CERTA-2002-AVI-081
Titre	Vulnérabilités dans Internet Explorer sous Mac OS
Date de la première version	17 avril 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-019
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 ;
- Exécution d'Apple Script.

## 2 Systèmes affectés

- Microsoft Internet Explorer 5.1 pour Macintosh OS X ;
- Microsoft Internet Explorer 5.1 pour Macintosh OS 8 et 9 ;
- Microsoft Outlook Express 5.0-5.03 pour Macintosh ;
- Microsoft Entourage v.X pour Macintosh ;
- Microsoft Entourage 2001 pour Macintosh ;
- Microsoft PowerPoint v.X pour Macintosh ;
- Microsoft PowerPoint 2001 pour Macintosh ;
- Microsoft PowerPoint 98 pour Macintosh ;
- Microsoft Excel v.X pour Macintosh ;
- Microsoft Excel 2001 pour Macintosh.

### **3 Description**

Deux vulnérabilités ont été découvertes sous Internet Explorer et la suite Office pour Macintosh :

Une vulnérabilité dans l'interprétation des éléments HTML permet à un concepteur de site mal intentionné de réaliser un débordement de mémoire lors de la visite d'une page HTML judicieusement composée, pouvant entraîner l'exécution de code arbitraire sur la machine cible. La suite Office utilisant les éléments HTML est également concernée par cette vulnérabilité.

Un concepteur de site mal intentionné peut, par le biais d'une page web judicieusement composée, exécuter un script sur la machine cible en utilisant Apple Script local. Ce script sera exécuté avec les droits de l'utilisateur.

Cependant le script doit déjà être présent sur la machine cible pour pouvoir être exécuté.

### **4 Solution**

Appliquer les correctifs disponibles selon votre configuration :

– MAC OS 8 et 9 :

<http://www.microsoft.com/mac/download>

– MAC OS X :

<http://www.apple.com/macosx/upgrade/softwareupdates.html>

### **5 Documentation**

Bulletin Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS02-019.asp>

## **Gestion détaillée du document**

**17 avril 2002** version initiale.