



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 20 mars 2003  
N° CERTA-2003-AVI-054

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Windows Script Engine

---

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-AVI-054>

---

### Gestion du document

Référence	CERTA-2003-AVI-054
Titre	Vulnérabilité de Windows Script Engine
Date de la première version	20 mars 2003
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS03-008
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.

## 2 Systèmes affectés

- Microsoft Windows 98 ;
- Microsoft Windows 98 Second Edition ;
- Microsoft Windows Me ;
- Microsoft Windows NT 4.0 ;
- Microsoft Windows NT 4.0 Terminal Server Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP.

## 3 Résumé

Une vulnérabilité de Windows Script Engine permet l'exécution de code arbitraire.

## **4 Description**

Windows Script Engine est un composant de Windows qui interprète et exécute les scripts écrits dans les langages tels que JScript, VBscript, ...

Un débordement de mémoire dans la bibliothèque qui gère les programmes de type JScript (*JScript.dll*) permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine de sa victime, par le biais d'une page web ou d'un mél au format HTML.

## **5 Contournement provisoire**

Désactiver l'exécution de scripts dans les navigateurs et les clients de courrier.

## **6 Solution**

Appliquer le correctif fourni par Microsoft (cf. section Documentation).

## **7 Documentation**

Avis de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS03-008.asp>

## **Gestion détaillée du document**

**20 mars 2003** version initiale.