

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Microsoft JScript

---

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-2006-AVI-241>

---

### Gestion du document

Référence	CERTA-2006-AVI-241
Titre	Vulnérabilité de Microsoft JScript
Date de la première version	14 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-023 du 13 juin 2006
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 ;
- déni de service.

## 2 Systèmes affectés

Les plates-formes suivantes sont affectées par la vulnérabilité :

- Microsoft Windows 2000 SP4 ;
- Microsoft Windows XP SP1, SP2 et x64 Edition ;
- Microsoft Windows XP x64 Edition ;
- Microsoft Windows 2003 Server sans et avec SP1 ;
- Microsoft Windows 2003 Server sans et avec SP1 pour processeurs Itanium ;
- Microsoft Windows 2003 Server x64 Edition ;
- Microsoft Windows 98, 98SE et Me ;

Les composants suivants sont affectés par la vulnérabilité :

- Microsoft JScript 5.1 sous Microsoft Windows 2000 SP4 ;
- Microsoft JScript 5.5 sous Microsoft Windows 2000 SP4 ;
- Microsoft JScript 5.6 sous Microsoft Windows XP SP1 et SP2 ;

- Microsoft JScript 5.6 sous Microsoft Windows XP x64 Edition ;
- Microsoft JScript 5.6 sous Microsoft Windows 2003 sans et avec SP1 ;
- Microsoft JScript 5.6 sous Microsoft Windows 2003 sans et avec SP1 pour processeurs Itanium ;
- Microsoft JScript 5.6 sous Microsoft Windows 2003 x64 Edition ;
- Microsoft JScript 5.6 sous Microsoft Windows 98, 98SE et Me.

### 3 Description

Une vulnérabilité dans Microsoft JScript permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable au moyen d'un script JScript malicieusement construit. L'exploitation de cette vulnérabilité peut se faire au moyen d'un message électronique ou un site Internet malicieux.

### 4 Contournement provisoire

- Désactiver le `Active Scripting`. Pour cela, dans l'onglet `Sécurité` des options Microsoft Internet Explorer, cliquer sur le bouton `Personnaliser le niveau...`, puis dans la section `Script et Active Scripting`, cocher `Désactiver` ;
- modifier la liste des contrôles d'accès (ACL) à la bibliothèque partagée `jscript.dll`. Pour cela, taper la commande `echo y|cacls %windir%/system32/jscript.dll /d everyone` puis relancer le navigateur ;
- utiliser un navigateur alternatif ;
- ne naviguer que sur des sites Internet de confiance.

### 5 Solution

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

### 6 Documentation

- Bulletin de sécurité Microsoft MS06-023 du 13 juin 2006 :  
<http://www.microsoft.com/france/technet/securite/MS06-023.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-023.msp>
- Référence CVE CVE-2006-1313 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1313>

### Gestion détaillée du document

14 juin 2006 version initiale.