



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 octobre 2004  
N° CERTA-2004-AVI-334

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans WebDAV

---

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-334>

---

### Gestion du document

Référence	CERTA-2004-AVI-334
Titre	Vulnérabilité dans WebDAV
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-030 de Microsoft
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

Déni de service.

## 2 Systèmes affectés

Les applications suivantes sont affectées :

- Internet Information Services 5.0 ;
- Internet Information Services 5.1 ;
- Internet Information Services 6.0.

sur les plates-formes :

- Microsoft Windows 2000 SP3 et SP4 ;
- Microsoft Windows XP et SP1 ;
- Microsoft Windows XP 64-Bit Edition SP1 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition.

### **3 Résumé**

Une vulnérabilité de type déni de service à été découverte dans WebDAV.

### **4 Description**

WebDAV (Web Distributed Authoring and Versioning) est une extension standardisée du protocole HTTP (Hypertext Transfer Protocol) permettant à plusieurs utilisateurs de travailler en coopération sur un serveur web.

L'interpréteur XML de Microsoft utilisé dans la mise en œuvre de WebDAV ne limite pas le nombre d'attributs pouvant être traités lors de la soumission de documents XML.

Un individu mal intentionné peut exploiter cette vulnérabilité afin d'effectuer un déni de service sur les versions des serveurs web Internet Information Server affectées grâce à l'envoi de requêtes HTTP judicieusement construites.

L'exploitation de cette vulnérabilité nécessite l'utilisation du service WebDAV.

### **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 MS04-030 du 12 octobre 2004 :  
<http://www.microsoft.com/technet/security/bulletin/ms04-030.msp>
- Référence CVE CAN-2003-0718 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0718>

## **Gestion détaillée du document**

**13 octobre 2004** version initiale.