

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Microsoft IIS 5.0

---

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-050>

---

### Gestion du document

Référence	CERTA-2003-AVI-050
Titre	Vulnérabilité de Microsoft IIS 5.0
Date de la première version	18 mars 2003
Date de la dernière version	–
Source(s)	Avis CA-2003-09 du CERT/CC
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.

## 2 Systèmes affectés

Microsoft IIS version 5.0 sous Windows 2000 avec Service Pack 3 et antérieurs.

## 3 Résumé

Une vulnérabilité dans un des composants du serveur Internet Microsoft IIS 5.0 permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

Le serveur Microsoft IIS 5.0 est fourni avec Windows 2000 par défaut. Il inclut le support du protocole WebDAV (Web Distributed Authoring and Versioning) qui permet la manipulation des fichiers du serveur IIS à distance. Un débordement de tampon dans la bibliothèque `ntdll.dll` permet à un utilisateur mal intentionné, via une requête malicieusement construite, d'exécuter du code arbitraire à distance.

## 5 Contournement provisoire

Voir article Microsoft 816930 :

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;816930>

## 6 Solution

Appliquer le correctif disponible sur le site de Microsoft :

<http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=fr>

## 7 Documentation

- Bulletin de sécurité Microsoft MS03-007 :  
<http://www.microsoft.com/technet/security/bulletin/ms03-007.asp>
- Article Microsoft 815021 :  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;815021>
- Article Microsoft 816930 :  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;816930>
- Alerte de sécurité ISS X-Force :  
<http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=22029>
- Avis de sécurité du CERT/CC CA-2003-09 :  
<http://www.cert.org/advisories/CA-2003-09.html>

## Gestion détaillée du document

**18 mars 2003** version initiale.