

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft IIS 4.0 et 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-2001-AVI-053>

---

### Gestion du document

Référence	CERTA-2001-AVI-053
Titre	Vulnérabilités dans Microsoft IIS 4.0 et 5.0
Date de la première version	15 mai 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-026
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 commandes à distance ;
- Accès aux données ;
- Déni de service.

## 2 Systèmes affectés

- Microsoft Internet Information Server 4.0 ;
- Microsoft Internet Information Server 5.0.

## 3 Résumé

Trois vulnérabilités ont été découvertes sous IIS 4.0 et 5.0.

La première vulnérabilité permet à un utilisateur distant d'exécuter des commandes sur le serveur cible. La seconde permet de se loguer en FTP, sous certaines conditions, sur un compte « invité » de l'un des domaines du réseau et la troisième permet d'entraîner un déni de service sur le serveur FTP.

## 4 Description

- Première vulnérabilité :  
Une fonctionnalité sous IIS permet de traiter les appels aux programmes de type CGI.  
Une vulnérabilité dans cette fonctionnalité permet à un utilisateur distant d'exécuter des commandes du système d'exploitation sur le serveur Web cible avec les privilèges du compte Web (compte IUSR\_[nom\_machine]). Elle lui fournit la possibilité de modifier des pages Web, d'ajouter ou de supprimer des fichiers, ou de reformater le disque dur.
- Seconde vulnérabilité :  
Dans le cas où un serveur FTP est membre d'un domaine NT ou Windows 2000, une vulnérabilité permet à un utilisateur distant mal intentionné d'ouvrir une connexion sur le serveur avec le compte « invité » et le mot de passe par défaut (souvent vide sur ce type de compte).
- Troisième vulnérabilité :  
Une vulnérabilité dans la gestion des requêtes sur un serveur FTP permet à un utilisateur distant, par le biais de caractères « joker », d'interrompre le serveur FTP par saturation de la mémoire.

## 5 Solution

Télécharger les correctifs sur le site Microsoft :

- Microsoft IIS 4.0 :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29787>
- Microsoft IIS 5.0 :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29764>

## 6 Documentation

Bulletin Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/ms01-026.asp>

## Gestion détaillée du document

15 mai 2001 version initiale.