

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans IIS

---

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-2010-AVI-434>

---

### Gestion du document

Référence	CERTA-2010-AVI-434
Titre	Vulnérabilités dans IIS
Date de la première version	15 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-065
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 à distance ;
- élévation de privilèges.

## 2 Systèmes affectés

IIS sur toutes les éditions de Windows XP, Vista, Seven, Server 2003 et Server 2008, et pour toutes les architectures.

## 3 Résumé

Plusieurs vulnérabilités affectent le serveur IIS. La plus grave permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

## 4 Description

Trois vulnérabilités du serveur IIS viennent d'être publiées :

- (CVE-2010-1899) le traitement défectueux de certaines URL par les serveurs IIS ASP est exploitable par un utilisateur malveillant pour provoquer un déni de service à distance ;
- (CVE-2010-2730) le traitement défectueux de certaines requêtes HTTP par les serveurs IIS 7.5 avec fonctionnalité FastCGI activée est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance ;
- (CVE-2010-2731) un défaut dans IIS 5.1 sur windows XP SP3 permet à un utilisateur malveillant de s'affranchir de l'authentification pour accéder à des ressources protégées.

## 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 MS10-065 du 14 septembre 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-065.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-065.msp>
- Référence CVE CVE-2010-1899 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1899>
- Référence CVE CVE-2010-2730 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2730>
- Référence CVE CVE-2010-2731 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2731>

## Gestion détaillée du document

15 septembre 2010 version initiale.