

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Internet Information Services

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-2008-AVI-077>

Gestion du document

Référence	CERTA-2008-AVI-077
Titre	Vulnérabilités dans Microsoft Internet Information Services (IIS)
Date de la première version	13 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-005 du 12 février 2008 Bulletin de sécurité Microsoft MS08-006 du 12 février 2008
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 ;
- élévation de privilèges.

2 Systèmes affectés

Les systèmes d'exploitation suivants sont affectés (utilisant Internet Information Services versions 5.0 à 7.0) :

- Windows 2000 SP4 (MS08-005) ;
- Windows XP SP2 (MS08-005, MS08-006) ;
- Windows XP Professionnel Edition x64 et Windows XP Professionnel Edition x64 SP2 (MS08-005, MS08-006) ;
- Windows Server 2003 SP1, Windows Server 2003 SP2 (MS08-005, MS08-006) ;
- Windows Server 2003 Edition x64 et Windows Server 2003 Edition x64 SP2 (MS08-005, MS08-006) ;
- Windows Server 2003 avec SP1 pour les systèmes Itanium et Windows Server 2003 avec SP2 pour les systèmes Itanium (MS08-005, MS08-006) ;
- Windows Vista et Windows Vista x64 (MS08-005).

3 Résumé

Deux vulnérabilités touchant *Microsoft Internet Information Services (IIS)* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance ou d'élever ses privilèges.

4 Description

Deux vulnérabilités affectent *Microsoft Internet Information Services* :

- La première vulnérabilité (MS08-005) concerne les services W3SVC, FTPSVC et NNTPSVC. Elle permet à une personne locale d'élever ses privilèges ;
- La deuxième vulnérabilité (MS08-006) concerne la façon dont *IIS* traite les entrées de données dans les pages web ASP. Une personne malintentionnée pourrait ainsi exécuter du code arbitraire à distance en envoyant des données spécialement conçues au serveur.

5 Solution

Se référer aux bulletins de sécurité MS08-005 et MS08-006 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-005 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-005.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-005.msp>
- Bulletin de sécurité Microsoft MS08-006 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-006.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-006.msp>
- Référence CVE CVE-2008-0074 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0074>
- Référence CVE CVE-2008-0075 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0075>

Gestion détaillée du document

13 février 2008 version initiale.