

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur FTP de Microsoft 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-2009-AVI-433>

Gestion du document

Référence	CERTA-2009-AVI-433
Titre	Vulnérabilités du serveur FTP de Microsoft IIS
Date de la première version	14 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-053 du 13 octobre 2009
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.

2 Systèmes affectés

- *Microsoft Internet Information Services (IIS) 5.0 (FTP Service 5.0) ;*
- *Microsoft Internet Information Services (IIS) 5.1 (FTP Service 5.1) ;*
- *Microsoft Internet Information Services (IIS) 6.0 (FTP Service 6.0) ;*
- *Microsoft Internet Information Services (IIS) 7.0 (FTP Service 7.0).*

3 Résumé

Deux vulnérabilités présentes dans le serveur FTP de *Microsoft IIS* permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité (CVE-2009-3023), de type débordement de mémoire, est présente dans le serveur FTP de *Microsoft IIS*. Elle permet à un utilisateur distant malintentionné de provoquer un déni de service sur les versions 5.1 et 6.0 et 7.0 ou d'exécuter du code arbitraire sur la version 5.0 du serveur vulnérable. Pour exploiter cette faille, l'attaquant doit disposer d'un compte ayant les droits d'écriture sur le serveur afin d'y créer des répertoires particuliers.

La deuxième vulnérabilité (CVE-2009-2521) est due à une saturation des ressources de la pile. Elle permet à une personne malintentionnée authentifiée de provoquer un déni de service au moyen d'une commande spécifique.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Document du CERTA CERTA-2009-ALE-015 du 01 septembre 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-015/index.html>
- Bulletin de sécurité Microsoft MS09-053 du 13 octobre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-053.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-053.msp>
- Référence CVE CVE-2009-2521 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2521>
- Référence CVE CVE-2009-3023 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3023>

Gestion détaillée du document

14 octobre 2009 version initiale.