Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

**S . G . D . S . N**
*Agence nationale de la sécurité des systèmes d'information*
*CERTA*

Paris, le 14 octobre 2009
N° CERTA-2009-ALE-015-004

**Affaire suivie par :**
CERTA

# BULLETIN D'ALERTE DU CERTA

## Objet : Vulnérabilités du serveur FTP de Microsoft IIS



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2009-ALE-015-004 |
| Titre | Vulnérabilités du serveur FTP de Microsoft IIS |
| Date de la première version | 01 septembre 2009 |
| Date de la dernière version | 14 octobre 2009 |
| Source(s) | Bulletin de sécurité VU#276653 de l'US-CERT |
| 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).

*Microsoft IIS* 7.5 n'est pas affecté. Les utilisateurs de *Microsoft IIS* 7.0 avec FTP Service 7.5 ne sont pas affectés.

## 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), due à une saturation des ressources de la pile, permet à une personne malintentionnée authentifiée de provoquer un déni de service au moyen d'une commande spécifique.

Du code permettant l'exploitation de ces vulnérabilités est disponible sur l'Internet.

# 5 Contournement provisoire

Pour la première vulnérabilité :

- Désactiver le support de l'écriture de fichiers dans la configuration du serveur FTP de *Microsoft IIS* pour les utilisateurs non identifiés (compte *anonymous*) ;
- supprimer la permission NTFS de créer des répertoires pour les utilisateurs du service ;

Pour les deux vulnérabilités :

- restreindre l'accès du serveur FTP aux seules personnes de confiance ;
- désactiver le service FTP si ce dernier n'est pas nécessaire ;
- utiliser un serveur FTP alternatif.

Les utilisateurs de *Microsoft Internet Information Services* 7.0 peuvent également mettre à jour le service FTP en version 7.5.

# 6 Solution

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

# 7 Documentation

- Bulletin de sécurité Microsoft MS09-053 du 13 octobre 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-053.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-053.mspx
- Bulletin de sécurité Microsoft 975191 du 01 septembre 2009 :
  http://www.microsoft.com/technet/security/advisory/975191.mspx
- Document du CERTA CERTA-2009-AVI-433 du 14 octobre 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-433/index.html
- Note de vulnérabilité de l'US-CERT VU#276653 du 31 août 2009 :
  http://www.kb.cert.org/vuls/id/276653
- 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

**01 septembre 2009** version initiale.

**02 septembre 2009** mise à jour des contournements provisoires, ajout des références au bulletin Microsoft et au CVE.

**04 septembre 2009** ajout de la référence CVE-2009-2521, ajout de IIS 7.0 dans la liste des produits vulnérables.

**07 septembre 2009** mise à jour des produits affectés, de la description des vulnérabilités et ajout d'un contournement provisoire.

**14 octobre 2009** ajout de la solution et des références correspondantes.