

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité WebDAV sous 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-ALE-007>

Gestion du document

Référence	CERTA-2009-ALE-007-002
Titre	Vulnérabilité WebDAV sous Microsoft IIS
Date de la première version	18 mai 2009
Date de la dernière version	10 juin 2009
Source(s)	
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- Microsoft Internet Information Services (IIS), pour les versions 5, 5.1 ou 6.0.

Microsoft Internet Information Services (IIS) 7.0 n'est pas affecté.

3 Résumé

Une vulnérabilité a été identifiée dans Microsoft IIS avec la fonctionnalité WebDAV. Elle permet à une personne malveillante distante de contourner la phase d'authentification et ainsi accéder (lire, charger et télécharger) à des fichiers arbitraires.

4 Description

Une vulnérabilité a été identifiée dans la gestion des en-têtes HTTP par le serveur Microsoft IIS avec la fonctionnalité WebDAV (*Web-based Distributed Authoring and Versioning*). Elle consiste en une mauvaise manipulation de caractères Unicode et peut être exploitée pour contourner la phase d'authentification et ainsi accéder (lire, charger et télécharger) à des fichiers arbitraires.

Du code d'exploitation est disponible sur l'Internet.

5 Contournement provisoire

Plusieurs contournements sont envisageables dans l'attente d'un correctif :

- si WebDAV n'est pas nécessaire, il doit être désactivé. C'est le cas par défaut sous IIS 6 ;
- restreindre l'accès Web aux machines de confiance ;
- filtrer les requêtes HTTP entrantes dont l'URL contient la chaîne %c0%af et l'en-tête HTTP présente l'information `Translate: f`. L'assistant IIS Lockdown et URLscan peuvent aider dans cette démarche, ainsi qu'une passerelle intermédiaire. Les méthodes inutiles doivent également être filtrées (PROPFIND par exemple). ;
- changer les droits d'accès (ACL) du système de fichiers pour l'utilisateur anonyme IUSR_[Nom-de-la-machine] ;
- migrer sous IIS 7 qui n'est pas, avec WebDAV, touché par cette vulnérabilité.

6 Solution

Se référer au bulletin de sécurité Microsoft MS09-020 pour l'obtention des correctifs (cf. section Documentation). Le CERTA a publié l'avis CERTA-2009-AVI-215 à ce sujet.

7 Documentation

- Avis CERTA-2009-AVI-215 du 10 juin 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-215/>
- Avis de sécurité Microsoft 971492 du 18 mai 2009 :
<http://www.microsoft.com/technet/security/advisory/971492.mspx>
- Bloc-notes Microsoft SRD, "More information about the IIS authentication bypass", 18 mai 2009 :
<http://blogs.technet.com/srd/archive/2009/05/18/more-information-about-the-iis-authentication-bypass.aspx>
- Référence CVE CVE-2009-1535 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1535>
- Page d'accueil Microsoft IIS :
<http://www.microsoft.com/windowsserver2003/iis/default.mspx>
- Avis du CERTA CERTA-2001-AVI-053 du 15 mai 2001 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-053/>
- Bloc-notes de T. Zoller, "IIS6 + WebDAV auth bypass and data upload", 16 mai 2009 :
<http://blog.zoller.lu/2009/05/iis-6-webdav-auth-bypass-and-data.html>
- Microsoft IIS Lockdown Tool :
<http://support.microsoft.com/kb/325864/fr>
<http://technet.microsoft.com/en-us/library/dd450372.aspx>
- Source d'informations sur WebDAV :
<http://www.webdav.org>
- Forum IIS, "Disable WebDAV protocol on IIS 6.0", mai 2008 :
<http://forums.iis.net/t/1149348.aspx>
<http://support.microsoft.com/kb/241520>

Gestion détaillée du document

18 mai 2009 version initiale.

19 mai 2009 ajout de la référence à l'avis de sécurité Microsoft associé.

10 juin 2009 ajout de la référence au bulletin de sécurité Microsoft MS09-020.