Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 février 2013
N° CERTA-2007-ALE-011-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité du composant d'indexation des serveurs Microsoft IIS

Gestion du document

Référence	CERTA-2007-ALE-011-002
Titre	Vulnérabilité du composant d'indexation des serveurs Microsoft IIS
Date de la première version	06 juin 2007
Date de la dernière version	19 février 2013
Source(s)	Alerte du SANS du 03 juin 2007
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 la confidentialité des données.

2 Systèmes affectés

Microsoft Internet Information Services (IIS) version 5.

3 Résumé

Une vulnérabilité a été découverte dans le composant d'indexation des serveurs `Microsoft IIS`. Elle permet d'accéder à des fichiers via un contournement de la politique d'authentification mise en place.

4 Description

Une vulnérabilité a été découverte dans le composant d'indexation (*Indexing Service*) des serveurs `Microsoft IIS`. Dans sa configuration par défaut, il est en effet possible d'accéder à des fichiers protégés ou au code source

des pages `asp` d'un tel serveur si la procédure d'authentification mise en place est de type « authentification basique » (*basic authentication*) ou authentification NTLM et si les droits NTFS le permettent.

En effet, le service d'indexation n'utilise pas les procédures d'authentification d'IIS pour accéder aux fichiers indexés mais celle du système de fichiers uniquement. Normalement, on pourrait se protéger de cela en requérant l'authentification basique ou NTLM voulue directement sur le fichier `.htw` qui est appelé pour afficher le contenu indexé. Toutefois, il existe un fichier virtuel `Null.htw` qui n'est pas configurable; dans la configuration par défaut, celui-ci peut donc être appelé par un utilisateur malveillant pour afficher du contenu indexé au moyen d'un requête spécialement construite.

Le composant d'indexation est installé par défaut dans `IIS 5`.

5 Contournement provisoire

Il est fortement conseillé de désinstaller ou de désactiver le service d'indexation.

Dans le cas contraire, d'autres contournements sont possibles :

- configurer le service d'indexation correctement pour qu'il n'utilise pas le fichier `Null.htw` et requérir l'authentification sur le fichier `.htw` utilisé ;
- mettre en oeuvre le contrôle de droits d'accès directement sur les fichiers et les répertoires du serveur, via les mécanismes d'ACL fournis par NTFS ;
- effectuer un filtrage des URLs afin de rendre inaccessible l'accès à des fichiers dont l'extension est `.htw` ;
- utiliser un serveur web alternatif.

Se référer au bulletin de sécurité de l'éditeur pour plus de détails.

6 Solution

La solution consiste à désinstaller ou à désactiver le service d'indexation et le surlignage des éléments correspondants. *Information Internet Services* version 5.0 (*IIS*) n'est plus supporté par Microsoft. La version 5.1 de *IIS* n'est pas impactée car le service d'indexation et le surlignage des éléments correspondants ne sont pas installés. La version 6.0 n'est pas impactée car le service d'indexation est installé mais le surlignage des éléments correspondants est désactivé. La version 7.0 est aussi non impactée car le service d'indexation n'est pas installé et le surlignage des éléments correspondants est désactivé lorsque le service d'indexation est installé.

7 Documentation

- Bulletin kb328832 de Microsoft du 05 juin 2007, mis à jour le 5 mars 2008 :
  http://support.microsoft.com/kb/328832
- Alerte du SANS du 03 juin 2007 :
  http://isc.sans.org/diary.html?storyid=2915
- Référence CVE CVE-2007-2815 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2815

Gestion détaillée du document

06 juin 2007 version initiale.

10 octobre 2008 mise à jour des produits affectés, de la description et du contournement provisoire.

19 février 2013 mise à jour des produits affectés et fermeture de l'alerte.