Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2006
N° CERTA-2006-AVI-388

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service d'indexage de Microsoft Windows

Gestion du document

Référence	CERTA-2006-AVI-388
Titre	Vulnérabilité dans le service d'indexage de Microsoft Windows
Date de la première version	13 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-053 du 12 septembre 2006
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professionnel Édition x64 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour les systèmes Itanium et Microsoft Windows Server 2003 avec SP1 pour les systèmes Itanium ;
- Microsoft Windows Server 2003 Édition x64.

3 Description

La plupart des versions de Microsoft Windows offrent un service d'indexage (*Indexing Service*) afin d'optimiser la recherche de fichiers à partir de certaines de leurs propriétés (noms, contenus, format, etc).

Ce service n'est pas lancé automatiquement par défaut, mais peut le devenir quand une personne choisit l'option «rendre les recherches futures plus rapides» au cours de l'une d'elles.

Le service sert aussi pour indexer le contenu des serveurs Web IIS (*Internet Information Services*).

Une vulnérabilité a été identifiée dans le service d'indexage. Associé à un serveur Web, il pourrait être utilisé par une personne malveillante pour une attaque de type `injection de code indirecte` (ou *cross-site scripting*). La vulnérabilité lui permettrait de modifier le contenu de certaines pages Web. Lorsqu'un utilisateur naviguerait sur le site compromis, la personne malveillante pourrait alors surveiller sa session Web, dérober des informations, ou exécuter d'autres codes sur le système de l'utilisateur.

4 Solution

Se référer au bulletin de sécurité MS06-053 de Microsoft pour l'application des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS06-053 du 12 septembre 2006 :
  http://www.microsoft.com/france/technet/security/bulletin/2006/MS06-053.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-053.mspx
- Référence CVE CVE-2006-0032 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0032

Gestion détaillée du document

13 septembre 2006 version initiale.