Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mai 2001
N° CERTA-2001-AVI-050

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le serveur d'indexation Windows

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-2001-AVI-050

Gestion du document

Référence	CERTA-2001-AVI-050
Titre	Vulnérabilités dans le serveur d'indexation Windows
Date de la première version	11 mai 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-025
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 ;
- Déni de service.

2 Systèmes affectés

- Microsoft Index Server 2.0 ;
- Indexing Service dans Microsoft Windows 2000.

3 Résumé

Une première vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire ou de créer un déni de service sur un serveur d'indexation 2.0.

Une seconde permet par le biais d'une vulnérabilité dans le service d'indexation de Windows 2000 de lire les fichiers résidant dans un serveur Web.

4 Description

- Première vulnérabilité (Microsoft Index Server 2.0):
  Le serveur d'indexation a pour but de retrouver rapidement certains fichiers sur une machine. Il est également utilisé dans certains sites Web.
  Un utilisateur mal intentionné peut, par le biais de requêtes spécifiques sur ce serveur, entraîner une exécution de code arbitraire avec les privilèges du serveur ou créer un déni de service.
- Deuxième vulnérabilité (Indexing Service dans Microsoft Windows 2000 et Microsoft Index Server 2.0) :
  Un utilisateur distant effectuant une requête sur des fichiers, relatifs au service d'index mais inexistants, peut découvrir l'architecture du répertoire relatif à IIS. Seul un accès en lecture est possible.

5 Contournement provisoire

Concernant la première vulnérabilité, une authentification NETBIOS préalable est nécessaire. Le fait de bloquer les ports NETBIOS au niveau du garde barrière permet d'empêcher la réalisation de cet exploit depuis internet, le risque se limitant à une attaque interne.

6 Solution

- Microsoft Index Server 2.0
  - Première vulnérabilité :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29660
  - Seconde vulnérabilité :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29631
- Indexing Service dans Microsoft Windows 200
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29561

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-025.asp

Gestion détaillée du document

11 mai 2001 version initiale.