

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le serveur d'indexation sous Microsoft

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-2000-AVI-090>

Gestion du document

Référence	CERTA-2000-AVI-090
Titre	Vulnérabilité dans le serveur d'indexation sous Microsoft
Date de la première version	20 décembre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft (MS00-098)
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

Accès aux données.

2 Systèmes affectés

- Index Server 2.0 ;
- Indexing Service 3.0.

3 Résumé

Un concepteur de site internet mal intentionné peut par le biais d'une requête ActiveX sur le serveur d'indexation, avoir connaissance des fichiers contenus dans le disque de la machine cible.

4 Description

Un contrôle ActiveX concernant l'indexation est inexactement marqué comme «reconnu sûr pour l'écriture de script». Cette vulnérabilité permet à un concepteur mal intentionné de site internet d'effectuer une requête afin

d'énumérer les fichiers et dossiers de la machine distante. Théoriquement cette vulnérabilité ne permet que la lecture des propriétés des fichiers (date de création, taille etc...), cependant par le biais de recoupement, il est possible d'établir la liste des caractères contenus dans les fichiers et reconstruire ainsi ces derniers.

Sur Windows 2000, ce serveur d'indexation est installé par défaut. Sur Windows NT4, il est installé seulement sur les machines comportant Internet Information Server.

5 Solution

Un correctif n'a seulement été publié que pour le service d'indexation 3.0 concernant Windows 2000. Microsoft jugeant que l'administrateur d'un système NT4 comportant lui-même un serveur internet (IIS) ne se sert pas de cette machine pour naviguer sur d'autres sites.

Correctif pour Indexing Service 3.0 (Windows 2000 - Version US) :
<http://www.microsoft.com/Download/Release.asp?ReleaseID=26595>

6 Documentation

Bulletin Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS00-098.asp>

FAQ Microsoft :
<http://www.microsoft.com/technet/security/bulletin/fq00-098.asp>

Gestion détaillée du document

20 décembre 2000 version initiale.