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 juin 2001
N° CERTA-2001-AVI-064

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le serveur d'indexation Windows

Gestion du document

Référence	CERTA-2001-AVI-064
Titre	Vulnérabilité dans le serveur d'indéxation Windows
Date de la première version	19 juin 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-33
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.

2 Systèmes affectés

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

3 Résumé

Une mauvaise gestion des URL par le module ISAPI idq.dll permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine cible.

4 Description

Le serveur d'indexation a pour but de retrouver rapidement certains fichiers sur une machine ainsi que sur certains sites Web.

Lors de l'installation d'Internet Information Server plusieurs modules ISAPI sont installés. Un de ces modules (idq.dll) est notamment un composant du serveur d'index.

Une mauvaise gestion de la mémoire de cette application permet à un utilisateur mal intentionné, par le biais d'une URL judicieusement composée, d'exécuter du code arbitraire sur la machine cible.

5 Contournement provisoire

Désactiver les configurations de scénario concernant la gestion des modules .idq et .ida dans le gestionnaire de service d'IIS.

6 Solution

Télécharger le correctif sur le site Microsoft :

- Windows NT 4.0 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
- Windows 2000 Professional, Server et Advanced Server :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800
- Concernant Microsoft Windows 2000 Datacenter Server, Microsoft préconise de prendre contact avec le fournisseur du serveur afin de connaître les solutions à apporter.

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Gestion détaillée du document

19 juin 2001 version initiale.