Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mai 2001
N° CERTA-2001-AVI-048

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft IIS 5.0

Gestion du document

Référence	CERTA-2001-AVI-048
Titre	Vulnérabilité dans Microsoft IIS 5.0
Date de la première version	02 mai 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-023
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

- Prise de contrôle d'un serveur ;
- Compromissions des données ;
- Exécution de code arbitraire.

2 Systèmes affectés

- Microsoft Windows 2000 Server ;
- Microsoft Windows 2000 Advanced Server ;
- Microsoft Windows 2000 Datacenter Server.

3 Résumé

Un débordement de mémoire tampon dans une extension ISAPI permet à un utilisateur mal intentionné de prendre le contrôle à distance d'un serveur IIS 5.0.

4 Description

Une extension ISAPI (IPP : Internet Printing Protocol) permet de contrôler via des requêtes HTTP les travaux d'impression. Cette extension est installée par défaut sur les serveurs Microsoft Server 2000.

Un utilisateur mal intentionné, par le biais d'une requête HTTP judicieusement composée, peut provoquer un débordement de la mémoire tampon de ce module dans le but de prendre le contrôle complet du serveur cible. N'importe quelle action peut alors être effectuée sur le serveur y compris l'installation de nouveaux programmes, la modification des pages HTTP ou la suppression de fichiers de données.

Le protocole IPP fonctionnant sur le principe d'une interface HTTP, cet exploit peut être effectué malgré la présence d'un garde barrière car seul le port 80 (HTTP) ou 443 (HTTPS) est sollicité.

Microsoft reconnait la gravité de cette vulnérabilité et préconise de mettre son système à jour très rapidement.

5 Contournement provisoire

Désactiver la fonction IPP dans l'extension ISAPI.

6 Solution

Télécharger le correctif sur le site Microsoft :

- Microsoft Windows 2000 Server et Microsoft Windows 2000 Advanced Server :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321
- 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 de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-023.asp

Gestion détaillée du document

02 mai 2001 version initiale.