Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 octobre 2000
N° CERTA-2000-AVI-061

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Internet Information Server sous Windows NT et 2000

Gestion du document

Référence	CERTA-2000-AVI-061
Titre	Vulnérabilité dans Internet Information Server sous Windows NT et 2000
Date de la première version	17 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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

- Modification d'un serveur web,
- accès avec privilèges,
- exécution de code arbitraire.

2 Systèmes affectés

Microsoft Internet Information Server 4.0 et 5.0 sous Windows NT et Windows 2000

3 Résumé

Une vulnérabilité dans Microsoft Internet Information Server permet à un visiteur mal intentionné d'usurper des privilèges qu'il n'a pas (accéder à n'importe quel fichier ou répertoire du volume contenant les pages web).

4 Description

Une erreur dans Internet Information Server permet à un visiteur mal-intentionné, en utilisant une URL habilement conçue, d'avoir accès à tous les fichiers et répertoires présents sur le volume contenant les pages web d'un serveur. Les privilèges qui lui sont accordés lors de cet accès, lui permettent d'exécuter des programmes sur la machine. Il pourrait, par conséquent, endommager fortement le serveur.

5 Contournement provisoire

Le compte servant à l'accès au site web par un visiteur est nommé `IUSR_nomdemachine` (où `nomdemachine` est le nom du serveur visité). Pour accéder au fichier d'un serveur web, cet utilisateur a les privilèges d'un utilisateur des groupes `tout le monde` et `utilisateurs`. Par défaut, la plupart des fichiers du système sont accessibles en lecture et exécution par ce groupe.

Supprimer cette autorisation d'accès aux fichiers du système empêchera à tout intrus sans privilèges spéciaux d'exécuter des commandes sur le système.

Pour augmenter la sécurité, le répertoire contenant les pages web du site doit être situé sur un volume différent de celui contenant le système du serveur.

6 Solution

Appliquer le correctif de Microsoft :

- Pour Windows 2000 :
  http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp
- Pour Windows NT :
  http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

Nota : Les administrateurs ayant déjà appliqué le correctif de Microsoft indiqué dans leur bulletin ms00-057 (Comme recommandé dans l'avis CERTA-2000-AVI-028) ont corrigé cette vulnérabilité en même temps, il n'est pas nécessaire d'appliquer celui-ci.

7 Documentation

- Bulletin de sécurité Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms00-078.asp
- La FAQ du bulletin de sécurité :
  http://www.microsoft.com/technet/security/bulletin/fq00-078.asp

Gestion détaillée du document

17 octobre 2000 version initiale.