Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 septembre 2000
N° CERTA-2000-AVI-044

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Windows NT4.0 affectant Internet Information Server

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-044

Gestion du document

Référence	CERTA-2000-AVI-044
Titre	Vulnérabilité de Windows NT4.0 affectant Internet Information Server
Date de la première version	07 septembre 2000
Date de la dernière version	–
Source(s)	Avis 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

Déni de service.

2 Systèmes affectés

Toute machine Windows NT 4.0. Le service Internet Information Server (IIS) est affecté, d'autres services pourraient l'être également.

3 Résumé

Un utilisateur mal intentionné peut, à l'aide d'une URL malformée, arrêter à distance le service IIS.

4 Description

Lorsqu'un utilisateur demande d'afficher cette URL malformée au serveur, le processus INETINFO.EXE consomme progressivement toutes les ressources du système (99-100% dans le gestionnaire des tâches).

Lorsque la mémoire virtuelle ne peut plus être étendue, le système tue (*kill*) le processus. Il se peut qu'une boîte de dialogue annonce que le système manque de mémoire virtuelle.

5 Solution

D'après Microsoft, la vulnérabilité ne provient pas du fonctionnement de l'application IIS, mais des systèmes Windows NT 4.0.

Il est donc recommandé d'appliquer ce correctif même si le serveur IIS n'est pas utilisé.

Appliquer le correctif pour les systèmes Windows NT 4.0 Workstation, Server et Server Enterprise Edition :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24079

Il n'existe pas encore de correctif pour Terminal Server Edition.

6 Documentation

- Le bulletin de sécurité de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms00-063.asp
- La FAQ sur le bulletin de sécurité de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/fq00-063.asp
- L'avis de sécurité de VIGILANTe aillant publié la vulnérabilité :
  http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2000009.htm

Gestion détaillée du document

07 septembre 2000 version initiale.