

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft 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-2002-AVI-124>

Gestion du document

Référence	CERTA-2002-AVI-124
Titre	Vulnérabilité de Microsoft Internet Information Server
Date de la première version	13 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-028 de 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Tous les serveurs Microsoft Internet Information Server 4.0 (Windows NT) et 5.0 (Windows 2000).

3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire à distance sur un serveur IIS 4.0 ou 5.0 grâce à un débordement de mémoire dans la gestion des scripts HTR.

4 Description

ISAPI (*Internet Services Application Programming Interface*) est une technologie permettant aux développeurs de site web de fournir des services plus ou moins élaborés par le biais d'une interface web.

L'extension ISAPI HTR est le prédécesseur des extensions ASP (*Active Server Pages*) permettant de gérer les mots de passe des utilisateurs de Windows NT à distance au moyen d'une interface web IIS.

Cette extension était installée par défaut sous IIS 2.0, et peut encore être installée sur les serveurs IIS 4.0 à 5.1 de façon à maintenir une compatibilité ascendante.

Le mécanisme de transfert des données engendrées par les scripts HTR est vulnérable aux débordements de mémoire.

Un utilisateur mal intentionné peut ainsi exécuter du code arbitraire à distance sur un serveur web IIS utilisant l'extension ISAPI HTR.

Le code sera exécuté dans le contexte de sécurité du compte `IWAM_Nom_de_machine` qui ne possède normalement pas de privilèges particuliers.

5 Contournement provisoire

Dans la mesure du possible désactiver les extensions HTR et leur préférer les extensions ASP.

6 Solution

Consulter le bulletin de sécurité MS02-028 de Microsoft (Voir paragraphe Documentation) pour connaître la disponibilité des correctifs.

7 Documentation

Bulletin de sécurité MS02-028 de Microsoft :

[HTTP://www.microsoft.com/technet/security/bulletin/MS02-028.ASP](http://www.microsoft.com/technet/security/bulletin/MS02-028.ASP)

Gestion détaillée du document

13 juin 2002 version initiale.