



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 août 2000
N° CERTA-2000-AVI-035

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft 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-035>

Gestion du document

Référence	CERTA-2000-AVI-035
Titre	Vulnérabilité dans Microsoft Information Server
Date de la première version	28 août 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

Exécution de code arbitraire.

2 Systèmes affectés

- Microsoft Internet Information Server 4.0 ;
- Microsoft Internet Information Server 5.0.

3 Résumé

Le 20 février 2000, le Cert CC a émis un avis concernant une vulnérabilité (Cross-Site Scripting) permettant à un utilisateur malveillant d'injecter du code dans la session d'un utilisateur d'un site internet. Microsoft vient de paraître un correctif pour cette vulnérabilité.

4 Description

Un utilisateur malveillant peut, par l'intermédiaire d'une requête (moteur de recherche, formulaire...) dirigée vers un serveur IIS, y insérer un script qui sera exécuté lors de la réponse à la requête. De ce fait, en invitant un utilisateur à cliquer sur un lien contenant ce type de requête, l'utilisateur malveillant peut faire exécuter du code sur la machine distante. Ce lien peut se trouver sur un site ou dans un courrier.

Nota : Selon Microsoft, de nombreux serveurs Web sont susceptibles d'être vulnérables à cette faille. Il est recommandé de prendre contact avec son fournisseur afin de savoir si un correctif existe.

5 Solution

Internet Information Server 4.0 :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseId=24000>

Internet Information Server 5.0 :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseId=23999>

6 Documentation

Bulletin de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS00-060.asp>

Faq Microsoft :

<http://www.microsoft.com/technet/security/bulletin/fq00-060.asp>

Gestion détaillée du document

28 août 2000 version initiale.