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 mars 2001
N° CERTA-2001-AVI-025

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilité d'Internet Information Server 5.0 et Exchange 2000**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2001-AVI-025 |
| Titre | Vulnérabilité d'Internet Information Server 5.0 et Exchange 2000 |
| Date de la première version | 02 mars 2001 |
| 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

- Déni de service ;
- Possibilité d'exécution de code arbitraire à distance.

## 2 Systèmes affectés

Internet Information Server 5.0 (IIS) et/ou Exchange 2000 en fonctionnement sur Windows NT ou 2000.

## 3 Résumé

Un mauvais traitement des URL envoyées au serveur IIS ou Exchange 2000 permet à un utilisateur mal intentionné de bloquer à distance le service HTTP.

## 4 Description

Un utilisateur mal intentionné peut, par le biais d'une URL habilement construite, effectuer un dépassement de mémoire, qui aura pour conséquence de bloquer à distance le service web.

Cette vulnérabilité est aussi présente sur Exchange 2000 car il est possible de traiter le courrier au travers d'une interface HTML.

Étant donné qu'il s'agit d'un dépassement de mémoire, il est possible d'exploiter cette vulnérabilité dans le but d'exécuter du code arbitraire sur le serveur victime.

# 5 Contournement provisoire

Pour Microsoft Exchange 2000 :

Si le traitement du mail au travers d'une interface HTML n'est pas nécessaire, désactiver cette fonction ou ne pas l'installer au départ.

# 6 Solution

Appliquer le correctif de Microsoft :

- Pour IIS 5.0 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=28155
- Pour Exchange 2000 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=28369

# 7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-014.asp

# Gestion détaillée du document

**02 mars 2001** version initiale.