



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2004
N° CERTA-2004-AVI-340

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Failles dans le service NNTP de Microsoft IIS

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-2004-AVI-340>

Gestion du document

Référence	CERTA-2004-AVI-340
Titre	Failles dans le service NNTP de Microsoft IIS
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS04-036
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 :
- exécution de code arbitraire à distance.

2 Systèmes affectés

Les systèmes d'exploitation Microsoft suivants sont concernés :

- Windows NT4 Serveur "Service pack" 6a
- Windows 2000 Serveur "Service packs" 3 et 4
- Windows 2003 Serveur (versions 32 comme 64 bits)
- Serveur Exchange 2000 "Service pack" 3
- Serveur Exchange 2003 avec et sans le "Service pack" 1

3 Résumé

Une vulnérabilité dans l'interprétation des requêtes NNTP permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

Le service Exchange nécessite l'installation du service NNTP. Un système peut donc être vulnérable même si il n'a pas vocation à offrir un service NNTP.

4 Description

NNTP est le protocole standard de gestion des groupes de discussion. Ce service est supporté par IIS sur les ports 119/tcp et éventuellement 563/tcp (connexions SSL/TLS).

Une faille a été identifiée dans la gestion d'une des requêtes du protocole. Cette dernière ne nécessite pas d'authentification préalable de l'utilisateur distant. Une mauvaise gestion d'un tampon dans la pile permet alors un déni de service ou l'exécution de code arbitraire sur la plateforme vulnérable.

5 Contournement provisoire

Désactiver le service NNTP dans IIS.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

– Bulletin de sécurité Microsoft MS04-036 du 12 octobre 2004 :

<http://www.microsoft.com/technet/security/bulletin/MS04-034.msp>

– Avis de sécurité de Core Security Technologies :

<http://www.coresecurity.com/common/showdoc.php?idx=420&idxseccion=10>

– Référence CVE CAN-2004-0574 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0574>

Gestion détaillée du document

13 octobre 2004 version initiale.