

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Exchange

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-066>

Gestion du document

Référence	CERTA-2000-AVI-066
Titre	Vulnérabilité de Microsoft Exchange
Date de la première version	02 novembre 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

Déni de service.

2 Systèmes affectés

Microsoft Exchange serveur 5.5 indépendamment de la plateforme.

3 Résumé

Une vulnérabilité dans la gestion des courriers entrants, permet à un courrier dont l'entête serait habilement construite d'arrêter le service de messagerie.

4 Description

Dans son fonctionnement normal, Microsoft Exchange 5.5 vérifie la validité des champs MIME dans l'entête des courriers entrants. Il traite de façon particulière les courriers dont l'entête est mal formée. Cependant le champ

MIME nommé « Content Type : », s'il est habilement construit échappe à ce traitement et bloque le service de messagerie.

5 Contournement provisoire

Quand cet incident se produit : redémarrer le service de messagerie Exchange, et supprimer le courrier ayant engendré l'erreur. Mais cette solution est très contraignante car elle implique la présence permanente d'un administrateur qui agirait manuellement sur le serveur pour le dépanner.

6 Solution

Il faut appliquer le correctif de Microsoft :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25443>

7 Documentation

<http://www.microsoft.com/technet/security/bulletin/ms00-082.asp>

<http://www.microsoft.com/technet/security/bulletin/fq00-082.asp>

Gestion détaillée du document

02 novembre 2000 version initiale.