

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Exchange Server 5.5

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-155>

Gestion du document

Référence	CERTA-2002-AVI-155
Titre	Vulnérabilité de Microsoft Exchange Server 5.5
Date de la première version	25 juillet 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-037 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

Microsoft Exchange Server 5.5.

3 Résumé

Une vulnérabilité de Microsoft Exchange Server permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

IMC (*Internet Message Connector*) est le nom donné au service SMTP de Microsoft Exchange Server.

Il est possible de réaliser un débordement de mémoire sur l'IMC lorsque ce dernier construit la réponse à la commande SMTP EHLO (*Extended HELLO*) dont le nom de domaine complet (FQDN pour *Fully Qualified domain*

Name) a été malicieusement construit. Ceci suppose que l'IMC consulte un serveur DNS (lors de la résolution de DNS inverse) dans lequel le FQDN en question a été enregistré.

5 Contournement provisoire

- Pour les serveurs Exchange n'utilisant pas le protocole SMTP, il est possible de désactiver le service IMC.
- Dans l'attente de l'application du correctif Microsoft, il est possible de désactiver l'utilisation de la résolution de DNS inverse par le serveur Exchange en modifiant comme suit une clé de la base de registre :
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters\
 1. Situer la valeur `DisableReverseResolve` ;
 2. dans le menu `Edit` cliquer sur `Binary` ;
 3. puis taper le chiffre «1».

6 Solution

Consulter le bulletin de sécurité MS02-037 de Microsoft pour connaître la disponibilité des correctifs.

7 Documentation

Bulletin de sécurité MS02-037 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS02-037.asp>

Gestion détaillée du document

25 juillet 2002 version initiale.