Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2004
N° CERTA-2004-AVI-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Exchange Server 2003

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-005

Gestion du document

Référence	CERTA-2004-AVI-005
Titre	Vulnérabilité de Microsoft Exchange Server 2003
Date de la première version	14 janvier 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS04-002
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

Elévation de privilèges.

2 Systèmes affectés

Microsoft Exchange Server 2003.

Les produits Microsoft Exchange 2000 Server et Microsoft Exchange Server 5.5 ne sont pas vulnérables.

3 Résumé

Une vulnérabilité de Microsoft Exchange Server 2003 permet à un utilisateur mal intentionné d'accèder à des informations non autorisées.

4 Description

Il est possible de déployer Exchange Server 2003 sur un serveur frontal, qui offre un accès Outlook Web Access (OWA) aux utilisateurs, et un ou plusieurs serveurs principaux, sur lesquels seront stockées les boîtes aux lettres.

Si l'authentification NTLM est utilisée pour les connexions HTTP entre le serveur frontal et un serveur principal, un utilisateur mal intentionné peut exploiter une vulnérabilité dans la gestion de ces connexions pour accèder à la boîte aux lettres d'un autre utilisateur.

Il faut pour cela que l'attaquant se soit authentifié au préalable au serveur frontal Exchange Server 2003, que les boîtes aux lettres de l'attaquant et de la victime soient sur le même serveur principal, et que la victime ait récemment accédé à sa boîte aux lettres.

De plus, l'exploitation de cette vulnérabilité est aléatoire, et la boîte aux lettres frauduleusement accédée ne peut pas être choisie.

5 Contournement provisoire

Il existe deux contournements provisoires.

- Désactiver la réutilisation des connexions HTTP sur le serveur frontal Exchange Server 2003. Cela peut éventuellement provoquer une baisse des performances si les clients utilisent OWA pour accèder à leurs boîtes aux lettres.
- Activer l'authentification Kerberos sur le serveur virtuel qui offre la fonctionnalité OWA sur le serveur principal Exchange Server 2003.

6 Solution

Appliquer le correctif proposé par Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms04-002.asp

7 Documentation

Avis de sécurité Microsoft MS04-002 :
http://www.microsoft.com/technet/security/bulletin/ms04-002.asp

Gestion détaillée du document

14 janvier 2004 version initiale.