Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 septembre 2001
N° CERTA-2001-AVI-092

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Exchange 5.5

Gestion du document

Référence	CERTA-2001-AVI-092
Titre	Vulnérabilité dans Microsoft Exchange 5.5
Date de la première version	07 septembre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-04
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

- Contournement des mécanismes de sécurité ;
- Accès à la liste des adresses méls d'un serveur Exchange 5.5.

2 Systèmes affectés

Microsoft Exchange 5.5.

3 Résumé

Un utilisateur distant mal intentionné peut contourner l'authentification demandée par Microsoft Exchange 5.5 afin de récupérer la liste complète des adresses méls des utilisateurs de ce serveur.

4 Description

Exchange 5.5 offre une particularité (Outlook Web Access -OWA-) permettant à des utilisateurs connus d'accèder à leur mél par l'intermédiaire d'un navigateur classique. OWA se comporte comme un serveur Web et autorise les utilisateurs à lire ou expédier du courrier sans passer par un logiciel de messagerie.

Pour la fonction de recherche, OWA fonctionne sur deux niveaux. Le premier effectuant l'authentification entre l'utilisateur et l'interface Web, le second permettant d'effectuer les recherches réelles sur les adresses méls des autres utilisateurs.

Une vulnérabilité située dans le second niveau permet à un utilisateur distant mal intentionné d'accéder directement au second niveau d'OWA sans s'authentifier, et de récupérer ainsi l'ensemble des adresses méls des utilisateurs connus par le serveur.

Microsoft Exchange 2000 n'est pas affecté par cette vulnérabilité.

5 Contournement provisoire

Si cette fonction n'est pas utilisée par vos utilisateurs, il est recommandé de la désactiver.

6 Solution

Télécharger le correctif sur le site Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32483

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-047.asp

Gestion détaillée du document

07 septembre 2001 version initiale.