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 décembre 2001
N° CERTA-2001-AVI-160

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'OWA dans Microsoft Exchange 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-2001-AVI-160

Gestion du document

Référence	CERTA-2001-AVI-160
Titre	Vulnérabilité d'OWA dans Microsoft Exchange 5.5
Date de la première version	07 décembre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-057
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.

2 Systèmes affectés

Microsoft Exchange 5.5.

3 Résumé

Un utilisateur mal intentionné peut, via la fonction OWA, manipuler la boîte aux lettres d'un utilisateur.

4 Description

Exchange 5.5 offre une particularité (Outlook Web Access -OWA-) permettant à des utilisateurs connus d'accèder à leurs méls 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.

Une vulnérablité présente dans OWA permet, lors de la lecture d'un message au format « HTML », d'exécuter automatiquement des scripts. Ainsi, si un utilisateur mal intentionné expédie un message de ce type à un destinataire utilisant la fonction OWA, le ou les scripts seront exécutés lors de la lecture. Ces scripts peuvent agir sur les méls présents et les modifier, les supprimer, etc.

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=34402

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-057.asp

Gestion détaillée du document

07 décembre 2001 version initiale.