

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel de messagerie Eudora 5.1 et versions antérieures

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-099>

Gestion du document

Référence	CERTA-2002-AVI-099
Titre	Vulnérabilité du logiciel de messagerie Eudora 5.1 et versions antérieures
Date de la première version	15 mai 2002
Date de la dernière version	–
Source(s)	Interne
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

- Divulgence d'informations sur le système ;
- perte de confidentialité.

2 Systèmes affectés

Eudora 5.1 et les versions précédentes sous Microsoft Windows.

Des expériences ont été effectuées sur Mac OS 9.x, mais elles n'ont pas permis de mettre en évidence cette vulnérabilité. Sous Mac OS X, Eudora est en cours de développement, il est donc impossible de vérifier la possibilité de l'exploitation de cette vulnérabilité actuellement.

Ceci n'exclut pas la possibilité d'utiliser une variante de cette vulnérabilité à l'encontre du logiciel sous Mac OS.

3 Résumé

Une vulnérabilité du logiciel de messagerie Eudora permet à un utilisateur mal intentionné d'obtenir n'importe quel fichier présent sur le système de sa victime.

4 Description

Eudora est un logiciel de messagerie compatible avec le protocole SMTP. Les messages reçus sont rangés dans des boîtes aux lettres (un fichier par boîte aux lettres), et toutes les pièces jointes sont placées dans un même répertoire (appelé *Attach* sous Windows et *Attachment Folder* sous Mac OS).

Il existe une vulnérabilité dans la gestion des balises servant à gérer les pièces jointes sous Eudora.

Un utilisateur mal intentionné peut obtenir n'importe quel fichier présent sur le système de sa victime si elle utilise le logiciel de messagerie Eudora en amenant cette dernière à renvoyer le message qu'il a habilement construit.

Il faut pour cela que l'attaquant connaisse l'emplacement sur le système du fichier qu'il désire obtenir, et qu'il pousse sa victime à lui renvoyer (fonction *forward*) son message.

5 Contournement provisoire

En plus de la vigilance quotidienne concernant la messagerie, tous les utilisateurs du logiciel de messagerie Eudora doivent surveiller le contenu des messages qu'ils renvoient afin de voir s'il y a eu insertion d'une pièce jointe non désirée à leur insu.

Il n'existe pas de correctif à ce jour.

Gestion détaillée du document

15 mai 2002 version initiale.