

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le client de messagerie électronique ELM

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-2005-AVI-321>

Gestion du document

Référence	CERTA-2005-AVI-321
Titre	Vulnérabilité dans le client de messagerie électronique ELM
Date de la première version	26 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Red Hat
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

ELM versions 2.5 PL5 à 2.5 PL7 (inclus).

3 Description

Une vulnérabilité de type débordement de pile dans la gestion des en-têtes SMTP de type `Expires` peut être utilisée par une personne distante mal intentionnée afin d'exécuter du code arbitraire par le biais d'un message électronique malicieusement construit.

Le code arbitraire s'exécute alors avec les droits de l'utilisateur destinataire du message électronique malicieux.

4 Solution

Mettre à jour le logiciel en installant la version 2.5 PL8 (cf. adresse du site de l'éditeur dans la partie Documentation).

5 Documentation

- Site de l'éditeur:
<http://www.instinct.org/elm/>
- Bulletin de sécurité de Red Hat :
<http://www.redhat.com/support/errata/RHSA-2005-755.html>
- Référence CAN-CVE : CAN-2005-2665
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2665>

Gestion détaillée du document

26 août 2005 version initiale.