

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du client de messagerie Pine

---

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-256>

---

### Gestion du document

Référence	CERTA-2002-AVI-256-002
Titre	Vulnérabilité du client de messagerie Pine
Date de la première version	02 décembre 2002
Date de la dernière version	13 janvier 2003
Source(s)	Avis de sécurité Linux SuSe : SuSe-SA:2002:046
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

Déni de service.

## 2 Systèmes affectés

Toutes les versions de `pine` strictement antérieures à la version 4.50.

## 3 Résumé

Une vulnérabilité dans le client de messagerie `pine` permet à un utilisateur mal intentionné de créer un déni de service.

## 4 Description

`pine` est un client de messagerie en mode texte. Lors de la réception d'un message électronique, `pine` n'alloue pas assez de mémoire nécessaire à l'analyse de l'adresse électronique de l'expéditeur. L'exploitation de cette vulnérabilité peut permettre à un utilisateur mal intentionné, envoyant un message électronique dont l'adresse source est habilement constituée, de créer un déni de service sur la machine qui reçoit le message.

## 5 Contournement provisoire

Il est possible de contourner provisoirement le problème en filtrant les entêtes des messages reçus avec un utilitaire de filtrage tel que `procmail`.

## 6 Solution

Mettre à jour le paquetage `pine` en version 4.50 (cf. section documentation).

## 7 Documentation

- Avis de sécurité de Linux SuSe : SuSe-SA:2002:046  
[http://www.suse.de/de/security/2002\\_046\\_pine.html](http://www.suse.de/de/security/2002_046_pine.html)
- Avis de sécurité de Mandrake Linux : MDKSA-2002:084  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:084>
- Avis de sécurité de RedHat Linux : RHSA-2002:270  
<http://rhn.redhat.com/errata/RHSA-2002-270.html>

## Gestion détaillée du document

**02 décembre 2002** version initiale.

**04 décembre 2002** ajout bulletin Mandrake.

**13 janvier 2003** ajout bulletin RedHat.