



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 mai 2004  
N° CERTA-2004-AVI-033-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du client de messagerie Mutt

---

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-2004-AVI-033>

---

### Gestion du document

Référence	CERTA-2004-AVI-033-001
Titre	Vulnérabilité du client de messagerie Mutt
Date de la première version	12 février 2004
Date de la dernière version	13 mai 2004
Source(s)	Bulletins 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 ;
- déni de service.

## 2 Systèmes affectés

- Versions de Mutt antérieures à la version 1.4.2 (stable) ;
- versions de Mutt antérieures à la version 1.3.28 (instable).

## 3 Résumé

Une vulnérabilité présente dans le client de messagerie Mutt peut être exploitée afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

## 4 Description

Mutt est un client de messagerie en mode texte très utilisé sur les plates-formes Linux. Il supporte les protocoles POP3 (Post Office Protocol) et IMAP (Internet Message Access Protocol) pour l'interrogation des serveurs de

messagerie.

Une vulnérabilité de type débordement de mémoire est présente dans Mutt.

Un utilisateur mal intentionné peut, par le biais d'un message électronique habilement constitué, exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance sur la plate-forme cliente avec les privilèges du compte utilisant l'application Mutt.

## 5 Solution

Les versions de Mutt 1.3.28 et postérieures ne sont pas vulnérables (branche instable).

Pour la branche stable, installer la version 1.4.2 de Mutt :

<http://www.mutt.org>

ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité RHSA-2004:050 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-050.html>
- Bulletin de sécurité RHSA-2004:051 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-051.html>
- Bulletin de sécurité MDKSA-2004:010 de Mandrake :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:010>
- Bulletin de sécurité FreeBSD du 12 février 2004 :  
<http://www.vuxml.org/freebsd>

## 6 Documentation

- Annonce de la version 1.4.2 sur le site de Mutt :  
<http://www.mutt.org/news.html>
- Référence CVE CAN-2004-0078 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0078>

## Gestion détaillée du document

**12 février 2004** version initiale.

**13 mai 2004** ajout du bulletin de sécurité FreeBSD.