

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de fetchmail

---

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-271>

---

### Gestion du document

Référence	CERTA-2002-AVI-271-003
Titre	Vulnérabilité de fetchmail
Date de la première version	18 décembre 2002
Date de la dernière version	31 janvier 2003
Source(s)	Avis de sécurité "Fetchmail remote vulnerability" d'e-matters Bulletin de sécurité RHSA-2002:293 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 ;
- déni de service.

## 2 Systèmes affectés

Toutes les versions de fetchmail antérieures ou égales à 6.1.3.

## 3 Résumé

Un débordement de mémoire dans fetchmail permet à un utilisateur mal intentionné de provoquer l'arrêt brutal ou l'exécution de code arbitraire avec les privilèges de l'utilisateur qui se sert de cette commande.

## 4 Description

Fetchmail est un utilitaire permettant de récupérer ses messages depuis un serveur de messagerie distant via divers protocoles (POP, IMAP...).

La routine réalisant l'allocation mémoire pour le traitement des adresses locales ne réserve pas suffisamment de place en mémoire. L'exploitation de cette vulnérabilité permet à un utilisateur mal intentionné de provoquer l'arrêt brutal de fetchmail ou l'exécution de code arbitraire avec les privilèges de l'utilisateur qui se sert de cette commande.

## 5 Solution

La version 6.2.0 corrige cette vulnérabilité.

Cette version est disponible sur le site :

<http://www.tuxedo.org/~esr/fetchmail>

## 6 Documentation

- "The fetchmail Home Page" :  
<http://www.tuxedo.org/~esr/fetchmail>
- Avis de sécurité "Fetchmail remote vulnerability" d'e-matters :  
<http://security.e-matters.de/advisories/052002.html>
- Avis de sécurité RHSA-2002:293 de RedHat :  
<http://rhn.redhat.com/errata/RHSA-2002-293.html>
- Avis de sécurité DSA-216 de Debian :  
<http://www.debian.org/security/2002/dsa-216>
- Avis de sécurité SuSE-SA:2003:001 de SuSE :  
[http://www.suse.com/de/security/2003\\_001\\_fetchmail.html](http://www.suse.com/de/security/2003_001_fetchmail.html)
- Bulletin de sécurité MDKSA-2003:011 de Mandrake :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:011>

## Gestion détaillée du document

**18 décembre 2002** version initiale.

**26 décembre 2002** ajout référence au bulletin de sécurité DSA-216 de Debian.

**6 janvier 2003** ajout référence au bulletin de sécurité SuSE-SA:2003:001 de SuSE.

**31 janvier 2003** ajout référence au bulletin de sécurité MDKSA-2003:011 de Mandrake.