

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-112>

Gestion du document

Référence	CERTA-2002-AVI-112
Titre	Vulnérabilité dans fetchmail
Date de la première version	29 mai 2002
Date de la dernière version	–
Source(s)	Avis de sécurité RHSA-2002:047 de RedHat
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

Toutes les versions de fetchmail antérieures à 5.9.10.

3 Résumé

Un débordement de mémoire dans la commande fetchmail permet à un utilisateur mal intentionné de provoquer 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 méls depuis un serveur de méls distant via divers protocoles (POP, IMAP...).

Lors de la récupération des méls depuis un serveur IMAP, fetchmail alloue une zone mémoire afin de stocker la taille des messages. La taille de cette zone mémoire dépend du nombre de méls à récupérer sur le serveur.

En annonçant un nombre de méls incorrect, un serveur malicieux peut provoquer un débordement de mémoire dans la commande fetchmail, pouvant entraîner l'exécution de code arbitraire avec les privilèges de l'utilisateur qui se sert de cette commande.

5 Solution

La version 5.9.10 corrige cette vulnérabilité.

Cette version est disponible sur le site :

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

6 Documentation

- Avis de sécurité RHSA-2002:047 de RedHat :
<http://rhn.redhat.com/errata/RHSA-2002-047.html>
- Avis de sécurité MDKSA-2002:0036 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-036.php>

Gestion détaillée du document

29 mai 2002 version initiale.