Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juin 2001
N° CERTA-2001-AVI-067

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-2001-AVI-067

Gestion du document

Référence	CERTA-2001-AVI-067
Titre	Vulnérabilité dans fetchmail
Date de la première version	27 juin 2001
Date de la dernière version	–
Source(s)	Avis de sécurité Debian DSA-060-1
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

Obtention du privilège root à distance.

2 Systèmes affectés

Toutes les versions de Fetchmail antérieures à 5.8.6.

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 unix permettant de récupérer ses mels depuis un serveur via les protocoles POP, IMAP...

Un champ `TO:` trop long inséré dans un message permet à un utilisateur mal intentionné de réaliser un débordement de mémoire et éventuellement de provoquer l'exécution d'un code arbitraire.

Le code arbitraire sera exécuté avec les privilèges de l'utilisateur se servant de la commande fetchmail.

5 Solution

La version 5.8.6 de fetchmail corrige le problème de dépassement de mémoire.
Cette version est disponible sur le site:
http://www.tuxedo.org/ esr/fetchmail

Se référer aux sites des différents distributeurs pour les mises-à-jour.

6 Documentation

Avis de sécurité Debian DSA-060-1

Gestion détaillée du document

27 juin 2001 version initiale.