Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 février 2010
N° CERTA-2010-AVI-050

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Fetchmail

Gestion du document

Référence	CERTA-2010-AVI-050
Titre	Vulnérabilité dans Fetchmail
Date de la première version	04 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Fetchmail fetchmail-SA-2010-01 du 04 février 2010
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 à distance.

2 Systèmes affectés

- Fetchmail 6.3.11 ;
- Fetchmail 6.3.12 ;
- Fetchmail 6.3.13.

3 Résumé

Une vulnérabilité affectant `Fetchmail` permet à un utilisateur distant de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans `Fetchmail` lorsqu'il est configuré en mode verbeux. Cette faille permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire par le biais d'un certificat au format `x509` construit de façon particulière.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de fetchmail :
  http://www.fetchmail.info
- Bulletin de sécurité Fetchmail fetchmail-SA-2010-01 du 04 février 2010 :
  http://mknod.org/svn/fetchmail/branches/BRANCH_6-3/fetchmail-SA-2010-01.txt
  http://www.fetchmail.info/fetchmail-SA-2010-01.txt

Gestion détaillée du document

04 février 2010 version initiale.