Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2007
N° CERTA-2007-AVI-020-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2007-AVI-020`

Gestion du document

Référence	CERTA-2007-AVI-020-003
Titre	Multiples vulnérabilités dans Fetchmail
Date de la première version	10 janvier 2007
Date de la dernière version	26 mars 2007
Source(s)	Bulletins de sécurité Fetchmail SA-2006-02 et SA-2006-03
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

- Déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Fetchmail versions 6.3.5 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans `Fetchmail` permettent à un utilisateur distant de provoquer un déni de service ou de porter atteinte à la confidentialité de données de connexions.

4 Description

Deux vulnérabilités sont présentes dans l'utilitaire de reccupération de mail `Fetchmail` :

- la première vulnérabilité est de type «pointeur nul» et permet à un utilisateur distant de provoquer un arrêt inopiné du service par le biais d'un message construit de façon particulière ;

– la deuxième vulnérabilité concerne un ensemble d'erreurs dans la mise en œuvre d'un certain nombre de systèmes d'authentification. Ces erreurs permettraient à un utilisateur distant de forcer `Fetchmail` à envoyer les données de connexions comme les mots de passe en clair plutôt qu'en chiffré comme indiqué dans son fichier de configuration.

5 Solution

La version 6.3.6 de `Fetchmail` corrige le problème :
http://fetchmail.berlios.de

6 Documentation

- Bulletin de sécurité `Fetchmail` SA-2006-02 du 04 janvier 2007 :
  http://fetchmail.berlios.de/fetchmail-SA-2006-02.txt
- Bulletin de sécurité `Fetchmail` SA-2006-03 du 04 janvier 2007 :
  http://fetchmail.berlios.de/fetchmail-SA-2006-03.txt
- Bulletin de sécurité RedHat RHSA-2007:0018 du 31 janvier 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0018.html
- Bulletin de sécurité Gentoo GLSA 200701-13 du 22 janvier 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200701-13.xml
- Bulletin de sécurité Mandriva MDKSA-2007:016 du 15 janvier 2007 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2007:016
- Bulletin de sécurité Debian DSA-1259 du 14 février 2007 :
  http://www.debian.org/security/2007/dsa-1259
- Bulletin de sécurité Ubuntu USN-405-1 du 11 janvier 2007 :
  http://www.ubuntu.com/usn/usn-405-1
- Bulletin de sécurité SuSE SUSE-SR:2007:004 du 16 mars 2007 :
  http://lists.suse.com/archive/suse-security-announce/2007-Mar/0005.html
- Référence CVE CVE-2006-5974 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5974
- Référence CVE CVE-2006-5867 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5867

Gestion détaillée du document

10 janvier 2007 version initiale.
29 janvier 2007 ajout des références aux bulletins de sécurité Gentoo, Mandriva et Ubuntu.
02 février 2007 ajout de la référence au bulletin de sécurité RedHat.
26 mars 2007 ajout des références aux bulletins de sécurité Debian et SuSE.