Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 octobre 2001
N° CERTA-2001-AVI-123

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans procmail

Gestion du document

Référence	CERTA-2001-AVI-123
Titre	Vulnérabilités dans procmail
Date de la première version	22 octobre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité RedHat RHSA-2001:093-03
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

Elévation de privilèges.

2 Systèmes affectés

Versions de procmail antérieures à la version 3.15.2. La version 3.15.2 n'est pas vulnérable.

3 Résumé

De multiples vulnérabilités présentes dans le code de gestion des signaux peuvent permettre à un utilisateur mal intentionné d'obtenir les droits de l'administrateur `root`.

4 Description

Procmail est un programme permettant de réaliser des traitements automatiques sur les méls (filtrage, réponse automatique, etc).

De multiples vulnérabilités présentes dans le code de gestion des signaux (code non réentrant), peuvent être exploitées par un utilisateur mal intentionné afin d'obtenir les droits de l'administrateur `root`.

Ces vulnérabilités ne sont exploitables qu'en local. Les privilèges `root` ne peuvent être obtenus que si la commande procmail est installée avec le drapeau `suid root` positionné, ce qui n'est pas le cas sur tous les systèmes.

5 Solution

Il est conseillé d'installer la dernière version de procmail disponible sur le site
http://www.procmail.org .
Certains éditeurs diffusent des paquetages pour leurs distributions (cf section Documentation).

6 Documentation

- Avis de sécurité RedHat : RHSA-2001:093-03;
- Avis de sécurité Debian : DSA 083-1;
- Avis de sécurité FreeBSD : FreeBSD-SA-01:60.

Gestion détaillée du document

22 octobre 2001 version initiale.