Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 août 2003
N° CERTA-2003-AVI-135

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur de messagerie Postfix

Gestion du document

Référence	CERTA-2003-AVI-135
Titre	Vulnérabilités du serveur de messagerie Postfix
Date de la première version	07 août 2003
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- balayage de ports par rebond («bounce scanning»).

2 Systèmes affectés

Tout système Unix utilisant Postfix, versions 1.1.12 et antérieures, comme serveur de messagerie.
Les versions courantes 2.x ne sont pas affectées.

3 Résumé

Il est possible pour un utilisateur distant mal intentionné de transmettre des messages volontairement mal rédigés qui permettent :

- de suspendre le service de messagerie (référence CVE CAN-2003-540) ;
- de tester tout port d'une adresse quelconque (éventuel contournement de la protection du réseau local par un pare-feu) ou d'utiliser le serveur comme agent d'un réseau de déni de service réparti (référence CVE CAN-2003-0468).

4 Description

Le code analysant les champs d'adresse («RCPT TO», «MAIL FROM» ou «Errors-To») peut être détourné au profit d'un utilisateur distant malveillant :

- pour les versions 1.1.9 à 1.1.12 et antérieures à 1.1.9 avec l'option «append_dot_mydomain» désactivée (activée par défaut), le service peut être suspendu jusqu'à l'effacement du ou des messages par l'administrateur ;
- pour les versions 1.1.11 et antérieures, le serveur peut tenter de se connecter à une adresse et un port arbitraire.

5 Solution

- Mettre à jour à partir des sources en version 1.1.13 au moins ou 2.x :
  http://www.postfix.org
- Debian Linux
  http://www.debian.org/security/2003/dsa-363
- Linux Mandrake
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:081
- Red Hat Linux
  http://www.redhat.com/support/errata/RHSA-2003-251.html
- SuSE Linux
  http://www.suse.de/de/security/2003_033_postfix.html

6 Documentation

- Référence CVE CAN-2003-0468
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0468
- Référence CVE CAN-2003-0540
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0540

Gestion détaillée du document

07 août 2003 version initiale.