



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 décembre 2001
N° CERTA-2001-AVI-162

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Déni de service potentiel de Postfix

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-162>

Gestion du document

Référence	CERTA-2001-AVI-162
Titre	Déni de service potentiel de Postfix
Date de la première version	17 décembre 2001
Date de la dernière version	–
Source(s)	Développeur du programme
Pièce(s) jointe(s)	Aucune

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

1 Risque

Déni de service sur le serveur de messagerie par épuisement de la mémoire disponible.

2 Systèmes affectés

Tout système Unix utilisant Postfix comme serveur de messagerie SMTP.

3 Résumé

Postfix est un des candidats, avec Qmail, au remplacement sécurisé du serveur SMTP Sendmail sur les systèmes Unix. Une erreur dans le code du serveur permettrait à un utilisateur mal intentionné de réaliser un déni de service à travers une simple connexion.

4 Description

Le serveur enregistre, afin de tracer les bogues, une copie des dialogues SMTP. Selon la configuration, celle-ci peut être envoyée à l'administrateur en cas d'erreur durant la session. Aucune limite n'est imposée à cet enregistrement, ce qui rend le serveur vulnérable à une attaque par saturation de ses ressources mémoires.

5 Solution

Mettre à jour le serveur.

- Sources
<ftp://ftp.porcupine.org/mirrors/postfix-release/index.html>
- Linux Mandrake
<http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-089.php3>
- Linux Red Hat
<http://archives.neohapsis.com/archives/bugtraq/2001-11/0239.html>
- Debian
<http://www.debian.org/security/2001/dsa-093>
- Conectiva Linux
<http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000439>

6 Documentation

- Message de Wietse Venema dans la liste de diffusion BugTraq
<http://archives.neohapsis.com/archives/bugtraq/2001-11/0107.html>

Gestion détaillée du document

17 décembre 2001 version initiale.