

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Policyd pour 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-2007-AVI-387>

---

### Gestion du document

Référence	CERTA-2007-AVI-387
Titre	Vulnérabilité de Policyd pour Postfix
Date de la première version	03 septembre 2007
Date de la dernière version	–
Source(s)	Note de mise à jour du projet Policy Daemon Mise à jour Debian DSA-1361-1 du 29 août 2007
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Les versions de Policy Daemon antérieures à 1.81.

Sous Debian, le module postfix-policyd a été corrigé dans la version 1.80-2.1etch1 (distribution Etch) et dans la version 1.80-2.2 (dans la distribution instable Sid).

## 3 Résumé

Une vulnérabilité a été identifiée dans le module anti-pourriel pour postfix, postfix-policyd, ou Policy Daemon. Il ne vérifierait pas correctement les commandes SMTP entrantes, ce qui permettrait à une personne malveillante d'exploiter par ce biais du code arbitraire sur le système.

## 4 Description

Une vulnérabilité a été identifiée dans le module anti-pourriel pour postfix, postfix-policyd, ou Policy Daemon. Il ne vérifierait pas correctement la longueur des commandes SMTP entrantes au niveau de la fonction `w_read()` de `socket.c`, ce qui permettrait à une personne malveillante d'exploiter par ce biais du code arbitraire sur le système.

## 5 Solution

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

## 6 Documentation

- Projet Policyd (Policy Daemon) pour Postfix :  
<http://www.policyd.org/changelog.html>
- Bulletin de sécurité Debian DSA 1361 du 29 août 2007 :  
<http://www.debian.org/security/2007/dsa-1361>
- Référence CVE CVE-2007-3791 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3791>
- Annonce de la version 1.81 de Policyd :  
[http://sourceforge.net/project/shownotes.php?release\\_id=522366](http://sourceforge.net/project/shownotes.php?release_id=522366)

## Gestion détaillée du document

03 septembre 2007 version initiale.