



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 août 2008
N° CERTA-2008-AVI-420

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2008-AVI-420>

Gestion du document

Référence	CERTA-2008-AVI-420
Titre	Vulnérabilités de Postfix
Date de la première version	19 août 2008
Date de la dernière version	–
Source(s)	CVE-2008-2936 et CVE-2008-2937
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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

Postfix dans les version suivantes :

- branche 2.3, avant la version 2.3.15 ;
- branche 2.4, avant la version 2.4.8 ;
- branche 2.5, avant la version 2.5.4 ;
- branche 2.6, avant la version 2.6-20080814.

3 Résumé

Deux vulnérabilités dans Postfix permettent à un utilisateur malveillant d'élever ses privilèges et de porter atteinte à l'intégrité et à la confidentialité de données.

4 Description

Le support des liens sur certains systèmes d'exploitation permet à un utilisateur malveillant de modifier des fichiers ne lui appartenant pas ou d'élever ses privilèges par la construction de liens et l'envoi de messages.

Un défaut de vérification des droits sur les boîtes aux lettres permet à un utilisateur malintentionné de lire des courriels qui ne lui sont pas destinés.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200808-12 du 14 août 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200808-12.xml>
- Bulletin de sécurité RedHat RHSA-2008:0839 du 14 août 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0839.html>
- Bulletin de sécurité OpenSuse SUSE-SA:2008:040 du 14 août 2008 :
<http://lists.opensuse-security-announce/2008-08/msg00002.html>
- Référence CVE CVE-2008-2936 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2936>
- Référence CVE CVE-2008-2937 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2937>

Gestion détaillée du document

19 août 2008 version initiale.