

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2011-AVI-146>

Gestion du document

Référence	CERTA-2011-AVI-146
Titre	Vulnérabilité dans Postfix
Date de la première version	10 mars 2011
Date de la dernière version	–
Source(s)	Bulletin de mise à jour Postfix du 7 mars 2011
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.

2 Systèmes affectés

- Postfix versions 2.7.x strictement inférieures à 2.7.3 ;
- Postfix versions 2.6.x strictement inférieures à 2.6.9 ;
- Postfix versions 2.5.x strictement inférieures à 2.5.12 ;
- Postfix versions 2.4.x strictement inférieures à 2.4.16.

3 Résumé

Une vulnérabilité dans la gestion du protocole TLS permet à un attaquant d'insérer des commandes dans les communications SMTP d'une victime.

4 Description

Il est possible à un attaquant en position d'interception (*man in the middle*) d'insérer des commandes SMTP lorsqu'un client souhaite utiliser une connexion sécurisée au moyen de la commande *STARTTLS*, qui est un message transmis en clair. Ces commandes sont alors interprétées par le serveur dans le contexte d'une connexion sécurisée.

5 Solution

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

6 Documentation

- Bulletin de mise à jour Postfix du 7 mars 2011 :
<http://www.postfix.org/announcements/postfix-2.7.3.html>
- Description détaillée de la vulnérabilité CVE-2011-0411 :
<http://www.postfix.org/CVE-2011-0411.html>
- Référence CVE CVE-2011-0411 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0411>

Gestion détaillée du document

10 mars 2011 version initiale.