

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-283>

Gestion du document

Référence	CERTA-2011-AVI-283-001
Titre	Vulnérabilité dans Postfix
Date de la première version	11 mai 2011
Date de la dernière version	19 mai 2011
Source	Bulletin de sécurité Postfix CVE-2011-1720 du 08 mai 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Postfix SMTP Server avec authentification SASL activée.

3 Résumé

Une vulnérabilité dans Postfix permet à un utilisateur malveillant de provoquer un déni de service à distance. La possibilité d'exécuter du code à distance n'est pas exclue.

4 Description

Lorsqu'un serveur SMTP Postfix utilise SASL, un défaut de gestion de l'authentification en fonction des connexions SMTP permet à un utilisateur malveillant de provoquer une corruption de la mémoire. Celle-ci provoque un arrêt inopiné du serveur. Il n'est pas exclu que l'attaquant puisse exécuter du code à distance avec les droits du compte système sous lequel le serveur SMTP s'exécute.

5 Solution

Les versions 2.5.13, 2.6.10, 2.7.4 et 2.8.3 du serveur SMTP Postfix corrigent ce problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Postfix CVE-2011-1720 du 08 mai 2011 :
<http://www.postfix.org/CVE-2011-1720.html>
- Référence CVE CVE-2011-1720 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1720>
- Bulletin de sécurité Fedora FEDORA-2011-6777 du 17 mai 2011 (postfix-2.7.4-1.fc13) :
<http://lists.fedoraproject.org/pipermail/package-announce/2011-May/060215.html>
- Bulletin de sécurité Fedora FEDORA-2011-6771 du 17 mai 2011 (postfix-2.7.4-1.fc14) :
<http://lists.fedoraproject.org/pipermail/package-announce/2011-May/060216.html>

Gestion détaillée du document

11 mai 2011 version initiale.

19 mai 2011 ajout des correctifs Fedora.