Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2011
N° CERTA-2011-AVI-655

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Dovecot

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-655

Gestion du document

Référence	CERTA-2011-AVI-655
Titre	Vulnérabilité dans Dovecot
Date de la première version	22 novembre 2011
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 2.0.16 de Dovecot
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.

2 Systèmes affectés

- Dovecot versions 2.0.15 et antérieures.

3 Résumé

Une vulnérabilité dans le serveur de messagerie Dovecot permet à un utilisateur malintentionné d'effectuer une attaque de type *Man in the middle*.

4 Description

Dans le cadre de l'utilisation d'un serveur Dovecot interconnecté à un serveur proxy au moyen d'une connexion SSL/TLS, le `Common Name` défini dans le certificat du serveur proxy n'est pas correctement vérifié. Cette vulnérabilité permet à un utilisateur malintentionné d'effectuer une attaque de type *Man-in-the-middle* sur la liaison SSL/TLS entre le serveur Dovecot et le serveur proxy.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La version 2.0.16 corrige le problème.

6 Documentation

– Liste des changements apportés à la version 2.0.16 de Dovecot :
http://www.dovecot.org/list/dovecot-news/2011-November/000200.html

Gestion détaillée du document

22 novembre 2011 version initiale.