Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 décembre 2011
N° CERTA-2011-AVI-722

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans pam_ssh sur FreeBSD

Gestion du document

Référence	CERTA-2011-AVI-722
Titre	Vulnérabilité dans pam_ssh sur FreeBSD
Date de la première version	26 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD du 23 décembre 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

Contournement de la politique de sécurité.

2 Systèmes affectés

– Toutes les versions de FreeBSD supportées.

3 Résumé

Une vulnérabilité dans *pam_ssh* permettant un contournement de la politique de sécurité a été corrigée.

4 Description

Si le module *pam_ssh* est activé, une personne malintentionnée peut être en mesure d'accéder aux comptes des utilisateurs qui n'ont pas chiffré leur clef privée *SSH*.

En effet l'appel à la bibliothèque *OpenSSL* pour déchiffrer les clefs privées ignore la « passphrase » passée en argument si la clef n'est pas chiffrée.

5 Solution

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

6 Documentation

– Bulletin de sécurité FreeBSD SA-11:09.pam_ssh du 23 décembre 2011 :
http://security.freebsd.org/advisories/FreeBSD-SA-11:09.pam_ssh.asc

Gestion détaillée du document

26 décembre 2011 version initiale.