



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 novembre 2006
N° CERTA-2006-AVI-485

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le module pam_ldap

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-2006-AVI-485>

Gestion du document

Référence	CERTA-2006-AVI-485
Titre	Vulnérabilité dans le module pam_ldap
Date de la première version	09 novembre 2006
Date de la dernière version	–
Source(s)	
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

- Mandriva 2006.0;
- Mandriva 2007.0;
- Mandriva CS4.0.

3 Résumé

PAM (Pluggable Authentication Module) est un système de gestion de la politique d'authentification. Parmi les modules, pam_ldap permet de gérer l'interface avec un annuaire ldap. Une vulnérabilité dans le module pam_ldap pourrait être exploitée afin de contourner la politique de sécurité en faussant la phase d'authentification.

4 Description

La vulnérabilité du module `pam_ldap` provoque une réponse positive de la fonction `pam_authenticate` même si l'authentification du client `pam_ldap` a échoué. Cette vulnérabilité permet donc à un attaquant de se connecter de façon illégitime.

5 Contournement provisoire

6 Solution

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

7 Documentation

- Bulletin de sécurité Mandriva MDKSA-2006:201 du 09 novembre 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:201>
- Référence CVE CAN-2006-5170 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-5170>

Gestion détaillée du document

09 novembre 2006 version initiale.