Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juillet 2005
N° CERTA-2005-AVI-245-002

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilités dans OpenLDAP, nss_ldap et 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-2005-AVI-245

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-AVI-245-002 |
| Titre | Vulnérabilités dans OpenLDAP, nss_ldap et pam_ldap |
| Date de la première version | 06 juillet 2005 |
| Date de la dernière version | 19 juillet 2005 |
| Source(s) | Bulletin de sécurité de OpenLDAP du 21 juin 2005 |
| 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 la confidentialité des données.

## 2 Systèmes affectés

- `OpenLDAP` versions 2.2.26 et antérieures ;
- `nss_ldap` versions 2.239 et antérieures ;
- `pam_ldap` versions 1.76 et antérieures.

## 3 Résumé

Une vulnérabilité dans `OpenLDAP`, `nss_ldap` et `pam_ldap` permet à un utilisateur local mal intentionné de porter atteinte à la confidentialité des données.

## 4 Description

`OpenLDAP` est un logiciel mettant en œuvre le protocole `LDAP (Lightweight Directory Access)`. `nss_ldap` est un service de nommage `NSS (Name Service Switch)` s'interfaçant avec un annuaire LDAP.

`pam_ldap` est un module d'authentification `PAM (Pluggable Layer Security)` s'interfaçant avec un annuaire `LDAP`. Une erreur dans la façon dont un serveur `LDAP` esclave redirige un client vers un serveur maître lors d'une connexion utilisant `TLS (Transport Layer Security)` permet à un utilisateur mal intentionné connecté au réseau local d'intercepter des informations de type identifiant et mot de passe.

# 5 Contournement provisoire

Configurer les serveurs `LDAP` pour qu'ils n'acceptent que des connexions en `LDAPS` et configurer les clients pour qu'ils utilisent des liens de type : *ldaps://*.

# 6 Documentation

- Bulletin de sécurité OpenLDAP du 21 juin 2005 :
  http://www.openldap.org/its/index.cgi/Incoming?id=3791
- Bulletin de sécurité Gentoo GLSA 200507-13 du 14 juillet 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200507-13.xml
- Bulletin de sécurité Mandriva MDKSA-2005:121 du 18 juillet 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:121
- Référence CVE CAN-2005-2069 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2069

# Gestion détaillée du document

**06 juillet 2005** version initiale.

**15 juillet 2005** ajout de la référence au bulletin de sécurité Gentoo 200507-13, correction de la référence CVE.

**19 juillet 2005** ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:121.