

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de nss-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-2009-AVI-127>

---

### Gestion du document

Référence	CERTA-2009-AVI-127
Titre	Vulnérabilité de nss-ldap
Date de la première version	02 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA 1758 du 30 mars 2009
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

nss-ldapd, version 0.6.7 et versions précédentes.

## 3 Résumé

Une vulnérabilité de nss-ldapd permet à un utilisateur malveillant de lire des informations sensibles.

## 4 Description

nss-ldapd permet l'utilisation d'un serveur LDAP pour le service NSS (*Name Service Switch*).

Une erreur de positionnement des droits sur un fichier de configuration permet à un utilisateur local de lire le mot de passe du serveur LDAP.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Debian DSA 1758 du 30 mars 2009 :  
<http://www.debian.org/security/2009/dsa-1758>
- Référence CVE CVE-2009-1073 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1073>

## **Gestion détaillée du document**

**02 avril 2009** version initiale.