Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 février 2011
N° CERTA-2011-AVI-092

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans OpenLDAP

Gestion du document

Référence	CERTA-2011-AVI-092
Titre	Multiples vulnérabilités dans OpenLDAP
Date de la première version	16 février 2011
Date de la dernière version	–
Source(s)	Rapports d'erreurs n6607 et n6661 de OpenLDAP
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

OpenLDAP versions 2.4.23 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans `OpenLDAP` permettent à un utilisateur malintentionné distant de contourner la politique de sécurité du système.

4 Description

Deux vulnérabilités sont présentes dans `OpenLDAP` :

– La première concerne le composant *back-ldap* et permet à un utilisateur distant de s'authentifier correctement malgré un mot de passe erroné. Pour être exploitable, il est nécessaire que les serveurs `OpenLDAP` maître et esclave soient configurés avec l'option *ppolicy_forward_updates*.

– la seconde est relative au composant *back-ndb* qui, sous certaines conditions, peut autoriser certaines actions sans authentification préalable. Afin de conduire une exploitation l'attaquant doit connaître le contenu de la directive *rootdn* présente dans le fichier *slapd.conf*.

5 Solution

La version 2.4.24 corrige ces problèmes :
http://www.openldap.org/software/download
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Site de OpenLDAP :
http://www.openldap.org
– Rapports d'erreurs n6607 et n6661 de OpenLDAP :
http://www.openldap.org/its/index.cgi/Software%20Bugs?id=6607
http://www.openldap.org/its/index.cgi/Software%20Bugs?id=6661

Gestion détaillée du document

16 février 2011 version initiale.