

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenLDAP

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-2012-AVI-147>

Gestion du document

Référence	CERTA-2012-AVI-147
Titre	Vulnérabilité dans OpenLDAP
Date de la première version	16 mars 2012
Date de la dernière version	–
Source(s)	Correction de bug OpenLDAP 7143
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

Déni de service à distance.

2 Systèmes affectés

OpenLDAP versions antérieures à 2.4.30.

3 Résumé

Une vulnérabilité a été corrigée dans OpenLDAP, qui permet de réaliser un déni de service à distance.

4 Description

Une vulnérabilité a été corrigée dans OpenLDAP. Elle peut être exploitée dans certaines conditions par un attaquant distant à l'aide d'une requête de recherche spécialement conçue.

5 Solution

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

6 Documentation

- Correction de bug OpenLDAP 7143 :
[http://www.openldap.org/its/index.cgi/Software Bugs?id=7143](http://www.openldap.org/its/index.cgi/Software+Bugs?id=7143)
- Référence CVE CVE-2012-1164 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1164>

Gestion détaillée du document

16 mars 2012 version initiale.