

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-2003-AVI-004>

Gestion du document

Référence	CERTA-2003-AVI-004-001
Titre	Vulnérabilité dans OpenLDAP
Date de la première version	16 janvier 2003
Date de la dernière version	7 février 2003
Source(s)	Bulletin de sécurité SuSE-SA:2002:047 de SuSE Bulletin de sécurité DSA-227 de Debian Bulletin de sécurité MDKSA-2003:006 de Mandrake
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

OpenLDAP version 2.0.25 et antérieures.

3 Description

OpenLDAP est une implémentation de LDAP (Lightweight Directory Access Protocol).

Plusieurs vulnérabilités présentes dans le paquetage OpenLDAP permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur une machine hébergeant un serveur LDAP vulnérable.

De plus, la bibliothèque OpenLDAP2 contient d'autres vulnérabilités exploitables en local.

4 Solution

Se référer aux bulletins de sécurité des différents éditeurs pour connaître la disponibilité des correctifs (cf. section Documentation).

5 Documentation

- Site de OpenLDAP :
<http://www.openldap.org>
- Bulletin de sécurité SuSE-SA:2002:047 de SuSE :
http://www.suse.com/de/security/2002_047_openldap2.html
- Bulletin de sécurité MDKSA-2003:006 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:006>
- Bulletin de sécurité DSA-227 de Debian :
<http://www.debian.org/security/2003/dsa-227>
- Bulletin de sécurité RHSA-2003:040 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-040.html>

Gestion détaillée du document

16 janvier 2003 version initiale.

7 février 2003 Ajout référence au bulletin de sécurité RHSA-2003:040 de Red Hat.