Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 décembre 2001
N° CERTA-2001-AVI-157

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'implémentations LDAP

Gestion du document

Référence	CERTA-2001-AVI-157
Titre	Multiples vulnérabilités d'implémentations LDAP
Date de la première version	03 décembre 2001
Date de la dernière version	–
Source(s)	Avis CA-2001-18 du CERT/CC
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 ;
- élévation de privilèges ;
- déni de service.

2 Systèmes affectés

- Netscape / iPlanet Directory Server version 5.0 Beta, version 4.13 et antérieures ;
- IBM SecureWay Directory sous Solaris et Windows 2000 version 3.2 et antérieures ;
- les versions de Lotus Domino R5 Server antérieures à 5.0.7a ;
- Microsoft Exchange 5.5 LDAP Service ;
- Oracle Internet Directory version 2.1.1.0.0 ;
- les versions d'OpenLDAP version 1.2.11 et antérieures et version 2.0.7 et antérieures.

3 Résumé

De nombreuses implémentations du protocole LDAP (Lightweight Directory Access Protocol) contiennent des vulnérabilités permettant à un utilisateur mal intentionné d'exécuter du code arbitraire, d'élever ses privilèges, ou de provoquer des dénis de service.

4 Description

4.1 Netscape / iPlanet Directory Server

Le code chargé de traiter les requêtes LDAP présente des vulnérabilités permettant à un utilisateur mal intentionné d'exécuter du code arbitraire avec les droits du *Directory Server* qui sont en général ceux de l'administrateur *root*.

Ces vulnérabiltés sont exploitables à distance.

4.2 IBM SecureWay Directory

Des vulnérabilités permettent à un utilisateur mal intentionné de provoquer un déni de service sur le serveur. Il est possible que ces vulnérabilités permettent en plus d'exécuter du code arbitraire.

Ces vulnérabilités sont présentes sous Solaris et Windows 2000, et sont exploitables à distance, mais les plates-formes Windows NT et AIX ne sont pas vulnérables.

4.3 Lotus Domino R5 Server

Des vulnérabilités permettent à un utilisateur distant d'exécuter du code arbitraire avec les privilèges du server Domino qui sont en général ceux de l'administrateur *root*.

4.4 Microsoft Exchange

Une vulnérabilité dans le traitement des requêtes LDAP rend les serveurs LDAP de Microsoft Exchange 5.5 vulnérables à un déni de service.

Cette vulnérabilité est exploitable à distance.

4.5 Oracle Internet Directory

De multiples vulnérabilités permettent à un utilisateur distant d'exécuter du code arbitraire avec les privilèges du serveur Keyserver qui sont en général ceux de l'administrateur *root*.

4.6 OpenLDAP

Une vulnérabilité du serveur OpenLDAP rend ce serveur vulnérable à un déni de service par arrêt (crash du serveur).

5 Contournement provisoire

Filtrez l'accès aux ports suivants pour limiter l'exploitation des vulnérabiltés :

- ldap 389/tcp
- ldap 389/ucp
  pour le protocole ldap (Lightweight Directory Access Protocol);

- ldaps 636/tcp
- ldaps 636/ucp
  pour le protocole ldaps (protocole ldap sur TLS/SSL - anciennement sldap).

6 Solution

Contactez votre revendeur pour obtenir une mise à jour :

- IBM :
  http://www.ibm.com/support
- Lotus Development Corporation :
  http://www.notes.net/qmrdown.nsf/qmrwelcome
- Microsoft :
  http://www.microsoft.com/support
- OpenLDAP Project :
  http://openLDAP.org/software/download

7 Documentation

- Avis de sécurité CA-2001-18 du Cert/CC :
  http://www.cert.org/advisories/CA-2001-18.html
- avis de sécurité Oracle :
  http://otn.oracle.com/deploy/security/pdf/oid_cert_bof.pdf
- avis de sécurité Debian DSA-068-1 ;
- avis de sécurité Mandrake MDKSA-2001:069 ;
- avis de sécurité RedHat RHSA-2001:098-05.

Gestion détaillée du document

03 décembre 2001 version initiale.