Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juin 2001
N° CERTA-2001-AVI-068

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de LDAP sous Microsoft Windows 2000

Gestion du document

Référence	CERTA-2001-AVI-068
Titre	Vulnérabilité de LDAP sous Microsoft Windows 2000
Date de la première version	27 juin 2001
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Microsoft MS01-036
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

Modification des mots de passe de n'importe quel utilisateur, dont l'administrateur du domaine Windows 2000.

2 Systèmes affectés

Windows 2000.

3 Résumé

L'implémentation de LDAP au travers de SSL dans Windows 2000 présente une vulnérabilité qui permet de modifier le mot de passe de n'importe quel utilisateur d'un domaine Windows 2000.

4 Description

LDAP (Lightweight Directiory Access Protocol) est un protocole standardisé permettant à un client d'interroger un annuaire situé sur un ou plusieurs serveurs. C'est l'un des protocoles utilisés dans Windows 2000 pour accéder à *Active Directory*.

Lorsqu'il est installé de façon à utiliser SSL, un utilisateur mal intentionné peut modifier le mot de passe personnel de n'importe quel utilisateur du domaine Windows.

Il peut faire ceci dans le but de rendre le compte de sa victime inaccessibles, ou bien dans le but de se connecter au domaine Windows auquel la victime appartient et d'obtenir ses privilèges. Il est notamment possible de modifier le mot de passe de l'`ADMINISTRATEUR` pour accéder à son compte et ses privilèges.

5 Contournement provisoire

Filtrer le port 636 (TCP) sur le garde-barrière permet de ne pas se faire attaquer depuis un réseau extérieur.

6 Solution

Appliquer au serveur LDAP sous SSL le correctif de Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31065

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-036.asp

Gestion détaillée du document

27 juin 2001 version initiale.