Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2009
N° CERTA-2009-AVI-213

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Active Directory

Gestion du document

Référence	CERTA-2009-AVI-213
Titre	Vulnérabilité dans Microsoft Active Directory
Date de la première version	10 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-018 du 09 juin 2009
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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Windows Server 2000 SP 4 ;
- Microsoft Windows XP Professionnel SP2 et SP3 (y compris pour l'Édition x64) ;
- Microsoft Windows Server 2003 SP2 (y compris pour les Éditions x64 et Itanium).

3 Résumé

Deux vulnérabilités ont été identifiées dans Microsoft Active Directory. L'exploitation de ces dernières peut provoquer un dysfonctionnement du service, voire l'exploitation de code à distance.

4 Description

Deux vulnérabilités ont été identifiées dans la mise en oeuvre des services d'annuaire Microsoft Active Directory :

- le service ne manipule pas correctement certaines requêtes LDAP ou LDAPS (*Lightweight Directory Access Protocol*). Cette vulnérabilité peut être exploitée à distance par le biais de trames spécialement construites afin de perturber le service, voire d'exécuter des commandes arbitraires sur le système vulnérable ;
- le service ne manipule pas correctement certaines requêtes LDAP ou LDAPS incluant des filtres OID (*Object Identifier*) particuliers. L'exploitation de cette vulnérabilité peut se faire à distance et provoque le dysfonctionnement du service.

5 Solution

Se référer au bulletin de sécurité Microsoft MS09-018 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-018 du 09 juin 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-018.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-018.mspx
- Référence CVE CVE-2009-1138 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1138
- Référence CVE CVE-2009-1139 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1139

Gestion détaillée du document

10 juin 2009 version initiale.