Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 octobre 2009
N° CERTA-2009-AVI-439

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Local Security Authority Subsystem Service

Gestion du document

Référence	CERTA-2009-AVI-439
Titre	Vulnérabilité dans Local Security Authority Subsystem Service
Date de la première version	14 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-059 du 13 octobre 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

Déni de service à distance.

2 Systèmes affectés

- Windows XP Service Pack 2 et Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 with SP2 pour systèmes Itanium ;
- Windows Vista, Windows Vista Service Pack 1, et Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition, Windows Vista x64 Edition Service Pack 1, et Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 pour systèmes 32-bit et Windows Server 2008 pour systèmes 32-bit Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32-bit ;

- Windows 7 pour systèmes x64 ;
- Windows Server 2008 R2 pour systèmes x64 ;
- Windows Server 2008 R2 pour systèmes Itanium.

3 Résumé

Une vulnérabilité dans le service *Local Security Authority Subsystem Service* (`LSASS`) permet à un utilisateur malintentionné de réaliser un déni de service à distance.

4 Description

Une vulnérabilité de type débordement d'entier dans le service *Local Security Authority Subsystem Service*, causée par une erreur dans le traitement de paquets malformés durant une procédure d'authentification `NTLM` (*NT Lan Manager*), peut être exploitée afin de provoquer un arrêt du service et le redémarrage du système.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS09-059 du 13 octobre 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-059.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-059.mspx
- Référence CVE CVE-2009-2524 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2524

Gestion détaillée du document

14 octobre 2009 version initiale.