Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 février 2005
N° CERTA-2005-AVI-051

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vunérabilté dans Microsoft Windows Licence Logging Service

Gestion du document

Référence	CERTA-2005-AVI-051
Titre	Vunérabilté dans Microsoft Windows Licence Logging Service
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-010
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 depuis un réseau local ;
- exécution de code arbitraire depuis un réseau local.

2 Systèmes affectés

- Microsoft Windows 2000 Server ;
- Microsoft Windows NT4.0 Server ;
- Microsoft Windows NT4.0 Server, édition Terminal Server ;
- Microsoft Windows Server 2003 édition Datacenter ;
- Microsoft Windows Server 2003 édition entreprise ;
- Microsoft Windows Server 2003 édition standard ;
- Microsoft Windows Server 2003 édition web.

3 Résumé

Une vulnérabilité présente dans le service d'enregistrement des licences sous Microsoft Windows permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter un code arbitraire sur le système ayant le service vulnérable activé.

4 Description

`Microsoft Windows Licence Logging Service (LLS)` est un service d'enregistrement des licences pour les serveurs Microsoft.

Kostya Kortchinsky du CERT Renater a découvert une vulnérabilité dans le service LLS qui peut être exploitée par un utilisateur mal intentionné du réseau local pour exécuter du code arbitraire sur le système ayant le service vulnérable. La vulnérabilité peut être exploitée par l'envoi d'un message malicieusement construit pour réaliser un débordement de mémoire sur le service vulnérable.

5 Solution

Se référer aux bulletins de sécurité des éditeurs (cf. section Documentation) pour l'obtention des correctifs.

6 Documentation

- Bulletin de sécurité Microsoft MS05-010 du 8 février 2005 :
  http://www.microsoft.com/technet/security/bulletin/ms05-010.mspx
- Référence CVE CAN-2005-0050 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0050

Gestion détaillée du document

09 février 2005 version initiale.