



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 janvier 2003
N° CERTA-2003-AVI-009

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans "Microsoft Locator Service"

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-009>

Gestion du document

Référence	CERTA-2003-AVI-009
Titre	Vulnérabilité dans "Microsoft Locator Service"
Date de la première version	23 janvier 2003
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS03-001
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows NT 4.0 ;
- Microsoft Windows NT 4.0 Terminal Server Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP.

3 Résumé

Une vulnérabilité présente dans Microsoft Locator Service permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine vulnérable ou d'entraîner un déni de service.

4 Description

Microsoft Locator Service est un service associant un nom logique à un identifiant réseau. Par défaut, ce service est uniquement activé sur les machines Contrôleur de domaine.

Un utilisateur mal intentionné peut, par le biais de paquets judicieusement composés, entraîner un déni de service ou exécuter du code arbitraire avec les droits `system`.

5 Contournement provisoire

Filtrer le port 135/TCP au niveau du garde-barrière.

6 Solution

Consulter le bulletin MS03-001 de Microsoft pour connaître la disponibilité des correctifs.

7 Documentation

Bulletin de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms03-001.asp>

Gestion détaillée du document

23 janvier 2003 version initiale.