Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 octobre 2003
N° CERTA-2003-AVI-168

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Messenger Service

Gestion du document

Référence	CERTA-2003-AVI-168
Titre	Vulnérabilité dans Microsoft Messenger Service
Date de la première version	16 octobre 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS03-043
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

- Elévation de privilèges ;
- Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows NT Workstation 4.0, Service Pack 6a ;
- Microsoft Windows NT Server 4.0, Service Pack 6a ;
- Microsoft Windows NT Server 4.0, Terminal Server Edition, Service Pack 6 ;
- Microsoft Windows 2000, Service Pack 2 ;
- Microsoft Windows 2000, Service Pack 3, Service Pack 4 ;
- Microsoft Windows XP Gold, Service Pack 1 ;
- Microsoft Windows XP 64-bit Edition ;
- Microsoft Windows XP 64-bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-bit Edition.

3 Résumé

Une vulnérabilité dans le service d'envoi de messages Microsoft (`Microsoft Messenger Service`) permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges `Local System`.

4 Description

`Microsoft Messenger Service` est un service permettant l'envoi de messages via NetBIOS ou RPC. Une vulnérabilité dans le service permet à un utilisateur mal intentionné de réaliser un débordement de tampon et ainsi exécuter du code arbitraire à distance avec les privilèges `Local System`.

5 Contournement Provisoire

- Filtrer les ports UDP 135, 137 et 138 et les ports TCP 135, 139 et 445 ;
- Désactiver le service `Microsoft Messenger Service`.

6 Solution

Appliquer le correctif fourni par Microsoft suivant la version du système d'exploitation (cf. Documentation).

7 Documentation

- Bulletin de sécurité MS03-043 de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/MS03-043.asp
- Référence CVE CAN-2003-0717 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0717

Gestion détaillée du document

16 octobre 2003 version initiale.