Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2003
N° CERTA-2003-AVI-185

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Windows Workstation Service

Gestion du document

Référence	CERTA-2003-AVI-185
Titre	Vulnérabilité dans Windows Workstation Service
Date de la première version	12 novembre 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS03-049
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 2000 Service Pack 2, Service Pack 3, Service Pack 4 ;
- Microsoft Windows XP ;
- Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition.

3 Résumé

Une vulnérabilité dans le service Windows Workstation Service permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans une fonction de gestion de journaux mise en oeuvre dans le service Workstation Service (WKSSVC.DLL). En exploitant cette vulnérabilité, un utilisateur mal intentionné peut réaliser un déni de service ou exécuter du code arbitraire à distance avec les privilèges `SYSTEM`.

5 Contournement provisoire

- Désactiver Windows Workstation Service (tout service dépendant de Windows Workstation Service ne fonctionnera plus, tel le partage de fichiers par exemple).
- Filtrer les ports TCP et UDP 138,139 et 445.

6 Solution

Appliquer le correctif fourni par Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS03-049.asp

7 Documentation

- Bulletin de sécurité Microsoft MS03-049 :
  http://www.microsoft.com/technet/security/bulletin/MS03-049.asp
- Avis de sécurité de Eeye AD20031111 :
  http://www.eeye.com/html/Research/Advisories/AD20031111.html
- Avis de sécurité du CERT/CC CA-2003-28 :
  http://www.cert.org/advisories/CA-2003-28.html
- Référence CVE CAN-2003-0812 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0812

Gestion détaillée du document

12 novembre 2003 version initiale.