Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 février 2001
N° CERTA-2001-AVI-023

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Dépassement de mémoire dans l'observateur d'événements de Windows 2000

Gestion du document

Référence	CERTA-2001-AVI-023
Titre	Dépassement de mémoire dans l'observateur d'événements de Windows 2000
Date de la première version	28 février 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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

Exécution de code arbitraire.

2 Systèmes affectés

Windows 2000

- Professional Edition
- Server
- Advanced Server
- Datacenter Server

3 Résumé

Une vulnérabilité de l'observateur d'événements (*Event Viewer*) de Windows 2000 permet à un utilisateur mal intentionné de bloquer l'observateur d'événements lorsqu'un utilisateur ouvre cet outil d'administration, voire exécuter du code arbitraire avec les privilèges de ce dernier.

4 Description

L'observateur d'événements est un outil de Windows 2000 (et Windows NT) permettant de dépouiller les journaux d'événements d'un de ces systèmes.

L'observateur d'événements ne peut pas être exécuté à distance. Il peut être manipulé par un utilisateur sans privilège pour les journaux `système` et `application` mais est le plus souvent utilisé par l'administrateur qui peut en plus visualiser le journal `sécurité`.

Il contient une fonction `détails` qui permet d'obtenir plus d'informations sur un événement particulier du journal observé.

Une vulnérabilité dans cette fonction permet à un utilisateur mal intentionné d'enregistrer un événement habilement construit (par un programme développé par ce dernier) qui fera déborder la pile lors de sa visualisation. Si c'est l'administrateur qui dépouille les journaux, l'événement construit peut exécuter du code avec les privilèges de celui-ci.

5 Solution

Appliquer le correctif Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=27842

Pour Windows 2000 Datacenter Server, les correctifs dépendent du matériel et sont à demander au fabriquant d'origine de la machine.

6 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-013.asp

Gestion détaillée du document

28 février 2001 version initiale.