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 juillet 2004
N° CERTA-2004-AVI-240-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Windows Task Scheduler

Gestion du document

Référence	CERTA-2004-AVI-240-001
Titre	Vulnérabilité dans Microsoft Windows Task Scheduler
Date de la première version	15 juillet 2004
Date de la dernière version	16 juillet 2004
Source(s)	Bulletin de sécurité Microsoft MS04-022
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 à distance.

2 Systèmes affectés

- Microsoft Windows 2000 Advanced Server ;
- Microsoft Windows 2000 Datacenter Server ;
- Microsoft Windows 2000 Professional ;
- Microsoft Windows 2000 Server ;
- Microsoft Windows XP Home Edition ;
- Microsoft Windows XP Professional ;
- Internet Explorer 6.0 Service Pack 1 installé sur Windows NT 4.0 SP6a.

3 Résumé

Une vulnérabilité dans Microsoft Windows Task Scheduler permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Un débordement de pile est présent dans la verification du nom de l'application à exécuter dans le gestionnaire de tâches (task scheduler `Mstask.dll`). Un utilisateur mal intentionné peut, via l'utilisation d'un email, d'un fichier ayant l'extension `.JOB` ou d'un site Internet malicieusement construit, réaliser un déni de service ou exécuter du code arbitraire sur la plate-forme vulnérable.

La vulnérabilité n'est exploitable que si la victime est administrateur du système.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS04-022 du 13 juillet 2004 :
  http://www.microsoft.com/technet/security/bulletin/ms04-022.mspx
- Bulletin de sécurité de l'US-CERT VU#228028 du 13 juillet 2004 :
  http://www.kb.cert.org/vuls/id/228028
- Référence CVE CAN-2004-0212 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0212

Gestion détaillée du document

15 juillet 2004 version initiale.

16 juillet 2004 correction des systèmes affectés et ajout du risque.