Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 avril 2007
N° CERTA-2007-AVI-169

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le noyau de Microsoft Windows

Gestion du document

Référence	CERTA-2007-AVI-169
Titre	Vulnérabilité dans le noyau de Microsoft Windows
Date de la première version	11 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-022 du 10 avril 2007
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows Server 2003 (Service Pack 1 et Service Pack 2 inclus) ;

3 Résumé

Une vulnérabilité a été identifiée dans le noyau de Microsoft Windows. Elle permettrait à une personne malveillante locale d'élever ses privilèges à ceux de l'administrateur.

4 Description

Une vulnérabilité a été identifiée dans le noyau de Microsoft Windows. La mise en œuvre du *Virtual DOS Machine* (`VDM`) aurait une situation de compétition (*race condition*) qui permettrait à une application d'accéder illégitimement aux premiers octets de la mémoire physique, aussi appelés `page zéro`, et donc d'élever les privilèges de l'utilisateur.

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 MS07-022 du 10 avril 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/MS07-022.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-022.mspx
- Bulletin de sécurité eEye AD20070410a du 10 avril 2007 :
  http://www.eeye.com/html/research/advisories/published/AD20070410a.html
- Référence CVE CVE-2007-1206 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1206

Gestion détaillée du document

11 avril 2007 version initiale.