Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 mars 2009
N° CERTA-2009-AVI-091

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le noyau Microsoft Windows

Gestion du document

Référence	CERTA-2009-AVI-091
Titre	Vulnérabilités dans le noyau Microsoft Windows
Date de la première version	10 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-006 du 10 mars 2009
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et 3 ;
- Microsoft Windows XP professional x64 Edition et x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 et 2, y compris les systèmes à base d'Itanium ;
- Microsoft Windows Vista et Service Pack 1 ;
- Microsoft Windows Vista x64 Edition et Service Pack 1 ;
- Microsoft Windows Server 2008 32-bit, x64 et à base d'Itanium.

3 Résumé

Plusieurs vulnérabilités dans le noyau Microsoft Windows permettent à une personne malveillante d'exécuter du code arbitraire à distance avec des privilèges élevés.

4 Description

Plusieurs vulnérabilités dans le noyau Windows ont été identifiées.

L'une des vulnérabilité, causée par un manque de contrôle des paramètres provenant de l'espace utilisateur, peut être exploitée au moyen d'un fichier au format `EMF` ou `WMF` spécialement construit afin d'exécuter du code arbitraire avec des privilèges élevés.

5 Solution

Se référer au bulletin de sécurité MS09-006 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-006 du 10 mars 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-006.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-006.mspx
- Référence CVE CVE-2009-0081 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0081
- Référence CVE CVE-2009-0082 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0082
- Référence CVE CVE-2009-0083 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0083

Gestion détaillée du document

10 mars 2009 version initiale.