Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 avril 2008
N° CERTA-2008-AVI-192

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Graphics Device Interface (GDI) de Windows

Gestion du document

Référence	CERTA-2008-AVI-192
Titre	Vulnérabilités dans Graphics Device Interface (GDI) de Windows
Date de la première version	09 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-021 du 08 avril 2008
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 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professionnel Édition x64 ;
- Microsoft Windows XP Professionnel Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 Édition x64 ;
- Microsoft Windows Server 2003 Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 avec SP1 pour les systèmes Itanium ;
- Microsoft Windows Server 2003 avec SP2 pour les systèmes Itanium ;
- Microsoft Windows Vista ;
- Microsoft Windows Vista Service Pack 1 ;
- Microsoft Windows Vista Édition x64 ;

– Microsoft Windows Vista Édition x64 Service Pack 1 ;
– Microsoft Windows Server 2008 pour systèmes 32 bits ;
– Microsoft Windows Server 2008 pour systèmes x64 ;
– Microsoft Windows Server 2008 pour systèmes Itanium.

3 Résumé

Deux vulnérabilités ont été identifiées dans Graphics Device Interface (GDI) de Windows. L'exploitation de ces dernières par le biais de fichiers image spécialement construits permettrait d'exécuter du code arbitraire à distance sur un système vulnérable.

4 Description

Deux vulnérabilités ont été identifiées dans Graphics Device Interface (GDI) de Windows. Il s'agit de l'interface permettant aux applications d'échanger des informations visuelles avec certains périphériques :

– GDI ne traite pas correctement le calcul d'entiers, notamment au cours de la manipulation de fichiers image aux formats `EMF` (*Enhanced Meta File*) et `WMF` (*Windows Metafile*).
– GDI ne manipule pas correctement les paramètres de nom de fichiers au format `EMF`, pouvant provoquer un débordement de pile.

L'exploitation de ces deux vulnérabilités par le biais de fichiers spécialement construits permettrait d'exécuter du code arbitraire à distance sur un système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS08-021 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité Microsoft MS08-021 du 08 avril 2008 :
http://www.microsoft.com/france/technet/security/Bulletin/MS08-021.mspx
http://www.microsoft.com/technet/security/Bulletin/MS08-021.mspx
– Référence CVE CVE-2008-1083 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1083
– Référence CVE CVE-2008-1087 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1087

Gestion détaillée du document

09 avril 2008 version initiale.