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 septembre 2008
N° CERTA-2008-AVI-449

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la bibliothèque Microsoft Windows GDI+

Gestion du document

Référence	CERTA-2008-AVI-449
Titre	Vulnérabilités dans la bibliothèque Microsoft Windows GDI+
Date de la première version	10 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-052 du 09 septembre 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

- les versions actuelles ddu système d'exploitation Microsoft Windows dont :
  - Windows XP SP2 et SP3 ;
  - Windows XP Professionnel Edition x64, SP2 inclus ;
  - Windows Server 2003 SP1 et SP2 ;
  - Windows Vista, SP1 inclus ;
  - Windows Server 2008.
- Internet Explorer 6 pour Windows 2000 SP4 ;
- Microsoft .NET Framework pour Windows 2000 SP4 ;
- Microsoft Office XP SP3 ;
- Microsoft Office 2003 SP2 et SP3 ;
- Microsoft Office 2007, SP1 compris ;
- Microsoft Visio 2002 SP2 ;
- Microsoft Office PowerPoint Viewer 2003 ;

- Microsoft Works 8 ;
- Microsoft Digital Image Suite 2006 ;
- SQL Server 2005 SP2 ;
- Microsoft Visual Studio .NET 2002 SP1 ;
- Microsoft Visual Studio .NET 2003 SP1 ;
- Microsoft Visual Studio 2005 SP1 ;
- Microsoft Visual Studio 2008 ;
- Microsoft Report Viewer 2005 et 2008 ;
- Microsoft Visual FowPro 8.0 et 9.0 ;
- Microsoft Platform SDK Redistribuable: GDI+ ;
- Microsoft Forefront Client Security 1.0.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans la bibliothèque graphique GDI+ de Microsoft. L'exploitation de ces dernières par le biais d'une image spécialement conçue peut provoquer l'exécution de code arbitraire sur un système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans la bibliothèque graphique GDI+ (`GdiPlus.dll`) de Microsoft :

- la bibliothèque ne gère pas correctement certaines informations concernant des grandeurs vectorielles ou gradients d'images basées sur du VML (*Vector Markup Language*) ;
- la bibliothèque ne manipule pas correctement des fichiers aux formats EMF, GIF et WMF. Cela peut entraîner une corruption de la mémoire.

5 Solution

Se référer au bulletin de sécurité MS08-052 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-052 du 09 septembre 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-052.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-052.mspx
- Bulletin de sécurité iDefense 743 du 09 septembre 2008 :
  http://www.idefense.com/ntelligence/vulnerabilities/display.php?id=743
- Référence CVE CVE-2007-5348 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5348
- Référence CVE CVE-2008-3012 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3012
- Référence CVE CVE-2008-3013 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3013
- Référence CVE CVE-2008-3014 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3014
- Référence CVE CVE-2008-3015 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3015

Gestion détaillée du document

10 septembre 2008 version initiale.