Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 septembre 2004
N° CERTA-2004-AVI-312-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GDI+ de Microsoft

Gestion du document

Référence	CERTA-2004-AVI-312-001
Titre	Vulnérabilité de GDI+ de Microsoft
Date de la première version	15 septembre 2004
Date de la dernière version	25 septembre 2004
Source(s)	BUlletin de sécurité MS04-028 de Microsoft
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 XP, Microsoft Windows XP SP1 ;
- Microsoft Windows XP 64-Bit Edition SP1, Microsoft Windows XP 64-Bit Edition 2003 ;
- Microsoft Windows server 2003, Microsoft Windows Server 2003 64-Bit Edition ;
- Microsoft Office XP SP3, Microsoft Office 2003 ;
- Microsoft Project 2002 SP1, Microsoft Project 2003 ;
- Microsoft Visio 2002 SP2, Microsoft Visio 2003 ;
- Microsoft Visual Studio .NET 2002 , Microsoft Visual Studio .NET 2003 ;
- Microsoft .NET Framework version 1.0 SDK SP2 ;
- Microsoft Picture IT! 2002, Microsoft Picture IT! version 7.0, Microsoft Picture IT! version 9.0 ;
- Microsoft Greetings 2002 ;
- Microsoft Digital Image Pro version 7.0, Microsoft Digital Image Pro version 9 ;
- Microsoft Digital Image Suite version 9 ;
- Microsoft Producer for Microsoft Office Powerpoint ;

– Microsoft Plateform SDK redistributable: GDI+ ;
– Internet Explorer 6 SP1 ;
– Microsoft .NET Framework version 1.0 SP2, Microsoft .NET Framework version 1.1.

Microsoft livre un outil, `GDI+ detection tool`, permettant de détecter la présence de logiciels installant le composant vulnérable sur un système.

NB : la liste ci-dessus des systèmes affectés n'est pas exhaustive. Il est possible que d'autres applications non référencées par Microsoft utilisent leur propre bibliothèque *gdiplus.dll* vulnérable.

3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans un des composants permettant le traitement des images au format JPEG peut être exploitée afin de réaliser l'exécution de code arbitraire sur un système vulnérable.

4 Description

`gdiplus.dll` est un composant graphique utilisé pour le traitement des images, le dessin vectoriel, etc. disponible en natif sur plusieurs système d'exploitation Windows ou installé avec certains logiciels Microsoft.

Une vulnérabilité de type débordement de mémoire est présente dans le composant `gdiplus.dll` lors du traitement des images au format JPEG. En incitant un utilisateur à visualiser une image au format JPEG habilement constituée, une personne mal intentionnée peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance sur une plate-forme vulnérable.

5 Solution

Les applications n'utilisent pas forcément la bibliothèque *gdiplus.dll* qui se trouve dans l'arborescence système de Windows. Il s'agit donc de corriger le fichier qui aurait pu être créé par l'installation de Windows, puis d'appliquer les correctifs pour toutes les applications vulnérables.

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

6 Documentation

– Bulletin de sécurité Microsoft MS04-028 du 14 septembre 2004 :
http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx
– Référence CVE CAN-2004-0200 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0200

Gestion détaillée du document

15 septembre 2004 version initiale.
25 septembre 2004 précision concernant les applicatifs tiers affectés par la vulnérabilité.