



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 septembre 2004  
N° CERTA-2004-ALE-011

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

**Objet : Diffusion de programmes exploitant la faille GDI+**

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-011>

---

### Gestion du document

Référence	CERTA-2004-ALE-011
Titre	Diffusion de programmes exploitant la faille GDI+
Date de la première version	23 septembre 2004
Date de la dernière version	–
Source(s)	
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 Platform SDK redistributable: GDI+ ;
- Internet Explorer 6 SP1 ;
- Microsoft .NET Framework version 1.0 SP2, Microsoft .NET Framework version 1.1.

### **3 Description**

Le CERTA a publié un avis en date du 15 septembre (CERTA-2004-AVI-312) concernant la vulnérabilité GDI+ de Microsoft.

De nombreux programmes exploitant cette vulnérabilité (*exploits*) sont actuellement disponibles sur l'Internet.

Le CERTA rappelle qu'il est indispensable d'appliquer les correctifs concernant les vulnérabilités des systèmes pour se protéger contre d'éventuelles attaques.

### **4 Solution**

Appliquer les correctifs proposés par l'éditeur.

### **5 Documentation**

Avis du CERTA CERTA-2004-AVI-312 du 15 septembre 2004 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-312/index.html>

## **Gestion détaillée du document**

**23 septembre 2004** version initiale.