

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans des composants graphiques de Microsoft Windows

---

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-2007-AVI-156>

---

### Gestion du document

Référence	CERTA-2007-AVI-156
Titre	Multiples vulnérabilités dans des composants graphiques de Microsoft Windows
Date de la première version	03 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-017 du 03 avril 2007
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 ;
- déni de service à distance ;
- élévation de privilèges.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition (SP2 inclus) ;
- Microsoft Windows Server 2003 (SP1 et SP2 inclus, ainsi que les versions pour les systèmes Itanium) ;
- Microsoft Windows Server 2003 x64 Edition (SP2 inclus) ;
- Microsoft Vista ;
- Microsoft Vista x64 Edition.

### 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans des composants graphiques de Microsoft Windows. Certaines sont largement exploitées actuellement, et ont fait l'objet des alertes CERTA-2007-ALE-002 et CERTA-2007-ALE-008. L'exploitation de ces dernières peut entraîner une élévation locale de privilèges, voire un déni de service ou l'exécution de code arbitraire à distance.

### 4 Description

Plusieurs vulnérabilités ont été identifiées dans des composants graphiques de Microsoft Windows. Parmi celles-ci :

- Windows ne manipulerait pas correctement les fichiers de formats de curseurs et d'icônes (reconnaissables par l'extension `.ani`). Cette vulnérabilité, largement exploitée, a fait l'objet de l'alerte CERTA-2007-ALE-008.
- L'ensemble de fonctions GDI (pour *Graphical Device Interface*) servant au traitement de fichiers graphiques, et plus précisément, son moteur de rendu Windows Graphics Rendering Engine, ne manipulerait pas correctement certains fichiers graphiques de type WMF (*Windows Metafile Format*) et EMF (*Enhanced Metafile Format*).
- GDI ne manipulerait pas correctement certaines tailles de fenêtres d'affichage. Cette vulnérabilité peut être exploitée par le biais d'une application malveillante, permettant ainsi une élévation de privilèges.
- GDI ne contrôlerait pas correctement certains paramètres liés à la coloration, ce qui pourrait provoquer un débordement de mémoire.
- Certaines polices de caractères ne seraient pas correctement interprétées par True Type Font Rasterizer, permettant à un utilisateur local de prendre le contrôle complet du système vulnérable.

### 5 Solution

Se référer au bulletin de sécurité MS07-017 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

### 6 Documentation

- Bulletin de sécurité Microsoft MS07-017 du 03 avril 2007 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS07-017.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-017.msp>
- Référence CVE CVE-2006-5586 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5586>
- Référence CVE CVE-2006-5758 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5758>
- Référence CVE CVE-2007-0038 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0038>
- Référence CVE CVE-2007-1211 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1211>
- Référence CVE CVE-2007-1212 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1212>
- Référence CVE CVE-2007-1213 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1213>
- Référence CVE CVE-2007-1215 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1215>
- Alerte CERTA-2007-ALE-002 du 12 janvier 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-002/>
- Alerte CERTA-2007-ALE-008 du 29 mars 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-008/>

# **Gestion détaillée du document**

**03 avril 2007** version initiale.