

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité VML du système 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-018>

---

### Gestion du document

Référence	CERTA-2007-AVI-018
Titre	Vulnérabilité VML du système Microsoft Windows
Date de la première version	09 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-004 du 09 janvier 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.

## 2 Systèmes affectés

- Internet Explorer 5.01 Service Pack 4 pour Microsoft Windows 2000 Service Pack 4 ;
- Internet Explorer 6 Service Pack 1 pour Microsoft Windows 2000 Service Pack 4 ;
- Internet Explorer 7 pour Microsoft Windows XP Service Pack 2 ;
- Internet Explorer 7 pour Microsoft Windows XP Professionnel Edition x64 ;
- Internet Explorer 7 pour Microsoft Windows Server 2003 et Server 2003 Service Pack 1 ;
- Internet Explorer 7 pour Microsoft Windows Server 2003 (Itanium) ;
- Internet Explorer 7 pour Microsoft Windows Server 2003 Edition x64.

## 3 Description

Une vulnérabilité a été identifiée dans la bibliothèque de gestion des documents au format VML (pour *Vector Markup Language*).

VML est un composant XML qui définit les caractéristiques d'images vectorielles. Il est mis en œuvre dans la bibliothèque `vgx.dll` de Microsoft Windows. La vulnérabilité concerne une mauvaise vérification du résultat de la multiplication de deux entiers, pouvant provoquer une saturation de mémoire tampon.

Cette vulnérabilité peut être exploitée par un utilisateur malintentionné afin d'exécuter du code arbitraire à distance sur une machine vulnérable par l'intermédiaire d'un document VML spécialement construit. Il peut par exemple insérer dans une page Web ou un courrier électronique au format HTML un tel document malveillant.

Cette mise à jour remplace le bulletin de sécurité MS06-055 du 26 septembre 2006.

## 4 Solution

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

## 5 Documentation

- Bulletin de sécurité Microsoft MS07-004 du 09 janvier 2007 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS07-004.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-004.msp>
- Avis du CERTA CERTA-2006-AVI-410 du 27 septembre 2006 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-410/>
- Référence CVE CVE-2007-0024 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0024>
- Bulletin de sécurité iDefense du 09 janvier 2007 :  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=462>

## Gestion détaillée du document

**09 janvier 2007** version initiale.