

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft Windows Authenticode Verification

---

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-2010-AVI-167>

---

### Gestion du document

Référence	CERTA-2010-AVI-167
Titre	Vulnérabilités dans Microsoft Windows Authenticode Verification
Date de la première version	14 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-019 du 13 avril 2010
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 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et 3 ;
- Microsoft Windows XP Professional x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 with SP2 pour système Itanium ;
- Microsoft Windows Vista, Vista Service Pack 1 et 2 ;
- Microsoft Windows Vista x64 Edition, Vista x64 Edition Service Pack 1 et 2 ;
- Microsoft Windows Server 2008 pour système 32-bit et Windows Server 2008 pour système 32-bit Service Pack 2 ;
- Microsoft Windows Server 2008 pour système x64 et Windows Server 2008 pour système x64 Service Pack 2 ;

- Microsoft Windows Server 2008 pour système Itanium et Windows Server 2008 pour système Itanium Service Pack 2 ;
- Microsoft Windows 7 pour système 32-bit ;
- Microsoft Windows 7 pour système x64 ;
- Microsoft Windows Server 2008 R2 pour système x64 ;
- Microsoft Windows Server 2008 R2 pour système Itanium.

### 3 Résumé

Deux vulnérabilités dans Microsoft Windows Authenticode Verification permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

### 4 Description

Deux vulnérabilités ont été découvertes dans Microsoft Windows Authenticode Verification et permettent à une personne malintentionnée d'exécuter du code arbitraire à distance :

- une vulnérabilité permet de modifier des portions de code d'un fichier exécutable ou *cabinet (.cab)* sans que sa signature ne soit invalidée (CVE-2010-0486). Cette vulnérabilité permet de prendre le contrôle total de la machine ;
- une vulnérabilité permet de modifier un fichier *cabinet (.cab)* existant, de le faire pointer sur une portion de code non vérifiée et de convaincre l'utilisateur d'ouvrir ou lire un fichier *cabinet* spécialement conçu (CVE-2010-0487). Cette vulnérabilité permet de prendre le contrôle total de la machine.

### 5 Solution

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

### 6 Documentation

- Bulletin de sécurité Microsoft MS10-019 du 13 avril 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-019.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-019.msp>
- Référence CVE CVE-2010-0486 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0486>
- Référence CVE CVE-2010-0487 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0487>

### Gestion détaillée du document

14 avril 2010 version initiale.