

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Windows CryptoAPI

---

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-2009-AVI-436>

---

### Gestion du document

Référence	CERTA-2009-AVI-436
Titre	Vulnérabilités dans Windows CryptoAPI
Date de la première version	14 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-056 du 13 octobre 2009
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 et Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 for Itanium-based Systems Service Pack 2 ;
- Windows Vista ;
- Windows Vista Service Pack 1 et Service Pack 2 ;
- Windows Vista x64 Edition ;
- Windows Vista x64 Edition Service Pack 1 et Service Pack 2 ;
- Windows Server 2008 for 32-bits Systems ;
- Windows Server 2008 for 32-bits Systems Service Pack 2 ;
- Windows Server 2008 for x64-based Systems ;

- *Windows Server 2008 for x64-based Systems Service Pack 2 ;*
- *Windows Server 2008 for Itanium-based Systems ;*
- *Windows Server 2008 for Itanium-based Systems Service Pack 2 ;*
- *Windows 7 for 32-bits Systems ;*
- *Windows 7 for 64-bits Systems ;*
- *Windows Server 2008 R2 for x64-based Systems ;*
- *Windows Server 2008 R2 for Itanium-based Systems.*

### **3 Résumé**

Deux vulnérabilités dans Windows CryptoAPI permettent un contournement de la politique de sécurité.

### **4 Description**

Deux vulnérabilités dans Windows CryptoAPI permettent d'usurper le certificat d'un site Web.

### **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 MS09-056 du 13 octobre 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-056.aspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-056.aspx>
- Référence CVE CVE-2009-2510 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2510>
- Référence CVE CVE-2009-2511 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2511>

## **Gestion détaillée du document**

**14 octobre 2009** version initiale.