

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans CAPICOM

---

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-208>

---

### Gestion du document

Référence	CERTA-2007-AVI-208
Titre	Vulnérabilité dans CAPICOM
Date de la première version	09 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-028 du 08 mai 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

- CAPICOM ;
- Platform SDK Redistributable: CAPICOM ;
- BizTalk Server 2004 Service Pack 1 ;
- BizTalk Server 2004 Service Pack 2.

## 3 Résumé

Une vulnérabilité dans CAPICOM permet l'exécution de code arbitraire à distance.

## 4 Description

Une vulnérabilité a été découverte dans *Cryptographic API Component Object Model* (CAPICOM). Elle affecte le contrôle ActiveX CAPICOM.Certificates. Un utilisateur malintentionné peut, par le biais d'un site

web ou d'un message électronique habilement constitué, exécuter du code arbitraire à distance sur la machine de sa victime.

## **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 MS07-028 du 08 mai 2007 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS07-028.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-028.msp>
- Référence CVE CVE-2007-0940 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0940>

## **Gestion détaillée du document**

**09 mai 2007** version initiale.