



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 14 février 2007  
N° CERTA-2007-AVI-086

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans ColdFusion

---

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-086>

---

### Gestion du document

Référence	CERTA-2007-AVI-086
Titre	Vulnérabilités dans ColdFusion
Date de la première version	14 février 2007
Date de la dernière version	–
Source(s)	Avis de sécurité d'Adobe APSB07-03 et APSB07-04
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

- Injection de code indirect.

## 2 Systèmes affectés

- ColdFusion MX 6.x;
- ColdFusion MX 7.x.

## 3 Résumé

Deux vulnérabilités sur ColdFusion permettent à un attaquant de réaliser une injection de code indirect (*cross-site scripting*).

## 4 Description

Deux vulnérabilités sur ColdFusion permettent à une personne malintentionnée de réaliser une injection de code indirect (*cross-site scripting*). La première vulnérabilité se trouve dans la page d'erreur par défaut de ColdFusion MX 6 et 7. La deuxième concerne les serveurs ColdFusion MX 7 qui n'ont pas activé le *Global Script Protection*.

## 5 Solution

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

## 6 Documentation

- Référence CVE CVE-2006-5859 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5859>
- Référence CVE CVE-2007-0817 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0817>
- Bulletin de sécurité Adobe APSB07-03 du 13 février 2007 :  
<http://www.adobe.com/support/security/bulletins/apsb07-03.html>
- Bulletin de sécurité Adobe APSB07-04 du 13 février 2007 :  
<http://www.adobe.com/support/security/bulletins/apsb07-04.html>

## Gestion détaillée du document

**14 février 2007** version initiale.