



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mars 2008
N° CERTA-2008-AVI-134

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Adobe 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-2008-AVI-134>

Gestion du document

Référence	CERTA-2008-AVI-134
Titre	Vulnérabilités dans Adobe ColdFusion
Date de la première version	13 mars 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité Adobe du 11 mars 2008
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 ;
- *Cross Site Scripting*.

2 Systèmes affectés

- Adobe ColdFusion 8 ;
- Adobe ColdFusion MX 7.

3 Résumé

Plusieurs vulnérabilités dans Adobe ColdFusion permettent à un utilisateur distant malintentionné de contourner la politique de sécurité ou de réaliser une attaque de type *cross site scripting*.

4 Description

Deux vulnérabilités dans certaines applications de ColdFusion, notamment celles mettant en œuvre la fonction `setEncoding` dans les fichiers `Application.chm` et `Application.cfc`, permettent à une personne malveillante de réaliser une attaque de type `cross site scripting`.

Une vulnérabilité dans Adobe ColdFusion permet de contourner la politique de sécurité appliquée à la journalisation des connexions à l'interface d'administration.

5 Solution

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

6 Documentation

- Bulletin de sécurité Adobe apsb08-06 du 11 mars 2008 :
<http://www.adobe.com/support/security/bulletins/apsb08-06.html>
- Bulletin de sécurité Adobe apsb08-07 du 11 mars 2008 :
<http://www.adobe.com/support/security/bulletins/apsb08-07.html>
- Bulletin de sécurité Adobe apsb08-08 du 11 mars 2008 :
<http://www.adobe.com/support/security/bulletins/apsb08-08.html>
- Référence CVE CVE-2008-0643 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0643>
- Référence CVE CVE-2008-0644 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0644>
- Référence CVE CVE-2008-1203 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1203>

Gestion détaillée du document

13 mars 2008 version initiale.