Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 décembre 2005
N° CERTA-2005-AVI-493

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans ColdFusion de Macromedia

Gestion du document

Référence	CERTA-2005-AVI-493
Titre	Multiples vulnérabilités dans ColdFusion de Macromedia
Date de la première version	19 décembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Macromedia MPSB05-12 du 15 décembre 2005 Bulletin de sécurité Macromedia MPSB05-14 du 15 décembre 2005
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Macromedia ColdFusion MX 6.0 ;
- Macromedia ColdFusion MX 6.1 ;
- Macromedia ColdFusion MX 6.1 avec JRun.

3 Résumé

De nombreuses vulnérabilités dans le serveur d'application ColdFusion permettent à un utilisateur distant mal intentionné de contourner la politique de sécurité ou de porter atteinte à la confidentialité des données.

4 Description

- Une vulnérabilité dans la fonction `Sandbox Security`, sur un système mettant en œuvre le serveur d'application ColdFusion avec JRun 4 de Macromedia, peut être exploitée par une personne mal intentionnée afin contourner la politique de sécurité et porter atteinte à la confidentialité des données ;
- une vulnérabilité dans le traitement du sujet d'un message électronique peut être exploitée pour contourner la politique de sécurité afin de joindre à ce message des fichiers arbitraires ;
- une vulnérabilité dans la fonction `CFOBJECT/CreateObject(Java)` peut être exploitée au moyen de classes Java malicieusement construites afin de contourner la politique de sécurité ;
- une vulnérabilité permet à un développeur mal intentionné de prendre connaissance du `hash` des mots de passe, au moyen d'un appel API (Application Programming Interface) malicieux.

5 Contournement provisoire

Pour les versions de ColdFusion MX 6.0 mettre à jour en passant à la version :

- ColdFusion MX 6.1 ;

Pour les versions de ColdFusion MX 6.1, appliquer le correctif disponible à l'adresse suivante :
http://download.macromedia.com/pub/security/mpsb05-12.zip

6 Solution

Appliquer la mise à jour de sécurité en passant à la version 7.0.1 de ColdFusion MX, disponible à l'adresse suivante :
http://www.macromedia.com/support/coldfusion/downloads_updates.html#mx7
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Macromedia MPSB05-12 du 15 décembre 2005 :
  http://www.macromedia.com/devnet/security/security_zone/mpsb05-12.html
- Bulletin de sécurité Macromedia MPSB05-14 du 15 décembre 2005 :
  http://www.macromedia.com/devnet/security/security_zone/mpsb05-14.html
- Mise à jour de sécurité ColdFusion MX 7.0.1 :
  http://www.macromedia.com/support/coldfusion/downloads_updates.html#mx7

Gestion détaillée du document

19 décembre 2005 version initiale.