Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 novembre 2002
N° CERTA-2002-AVI-247

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de JRun et ColdFusion pour Microsoft IIS

Gestion du document

Référence	CERTA-2002-AVI-247
Titre	Vulnérabilités de JRun et ColdFusion pour Microsoft IIS
Date de la première version	15 novembre 2002
Date de la dernière version	–
Source(s)	bulletin de sécurité Macromedia
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

- Elévation de privilèges ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- ColdFusion MX (version 6.0 et antérieures) pour IIS 4.0 et 5.0 sous Windows ;
- JRun 3.0, 3.1 et 4.0 pour IIS sous Windows.

3 Résumé

Il existe une vulnérabilité de type débordement de mémoire exploitable à distance dans les applications ColdFusion et JRun pour IIS sous Windows.

4 Description

ColdFusion et JRun sont des applications crées par Macromedia utilisant la technologie `ISAPI` (*Internet Services Application Programming Interface*) et permettant de développer des extensions pour les serveurs web. ISAPI est une technologie permettant aux développeurs de site web de fournir des services plus ou moins élaborées par le biais d'une interface web.

Le filtre ISAPI gérant les noms de fichier possède une vulnérabilité de type débordement de mémoire.

Un utilisateur mal intentionné peut, en utilisant des noms de fichiers très longs, exécuter du code arbitraire sur le serveur IIS avec les privilèges très élevés de l'utilisateur `SYSTEM`.

5 Solution

Se référer aux bulletins de sécurité Macromedia (voir paragraphe documentation) pour connaître la disponibilité des correctifs.

`Nota` : Le correctif de JRun est un correctif cumulatif qui corrige d'autres erreurs.

Le `Service Pack 1` et le `Service Pack 1a` pour JRun corrigent les vulnérabilités couvertes par le correctif cumulatif. Ce dernier ne doit donc pas être appliqué si l'un de ces `Service Pack` a été installé.

6 Documentation

- Bulletin de sécurité de Macromedia concernant ColdFusion :
  http://www.macromedia.com/v1/handlers/index.cfm?ID=23161
- Bulletin de sécurité de Macromedia concernant JRun :
  http://www.macromedia.com/v1/handlers/index.cfm?ID=23500

Gestion détaillée du document

15 novembre 2002 version initiale.