Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 septembre 2004
N° CERTA-2004-AVI-327

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans JRUN Server

Gestion du document

Référence	CERTA-2004-AVI-327
Titre	Multiples vulnérabilités dans JRUN Server
Date de la première version	27 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MPSB04-08 de Macromédia
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 ;
- contournement de la politique de sécurité ;
- usurpation de session ;
- déni de service.

2 Systèmes affectés

JRUN versions 3.0, 3.1 et 4.0.

3 Description

JRUN est un serveur applicatif présent dans les serveurs web les plus courants (Apache et Internet Information Server (IIS)). Plusieurs vulnérabilités affectent ce serveur :

- Une vulnérabilité dans la génération et la manipulation de l'identifiant de sessions `JSESSIONID` du serveur JRUN permet à un utilisateur mal intentionné d'usurper une session entre un client et le serveur vulnérable ;
- une vulnérabilité de type `Cross-site scripting` est présente dans la console d'administration JRUN Management Console ;

– une vulnérabilité présente dans le connecteur JRUN du serveur Web Internet Information Server de Microsoft permet à un utilisateur mal intentionné, au moyen d'une URL malicieusement construite, de contourner les restrictions d'accès appliquées à certaines pages web (possèdants les extentions .php, .asp et .pl) afin d'en visualiser le code source ;
– une vulnérabilité du serveur JRUN permet à un individu mal intentionné d'éxecuter du code arbitraire à distance afin de provoquer l'arrêt de la machine lorsque celle-ci est configurée en mode de débogage.

Les trois premières vulnérabilités affectent uniquement la version 4.0 du serveur JRUN.

4 Solution

Appliquer le correctif de sécurité disponible à partir du site de l'éditeur (cf. Documentation).

5 Documentation

Bulletin de sécurité MPSB04-08 de Macromédia :
http://www.macromedia.com/devnet/security/security_zone/mpsb04-08.html

Gestion détaillée du document

27 septembre 2004 version initiale.