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 septembre 2011
N° CERTA-2011-AVI-504

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilités dans Spring Framework**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2011-AVI-504 |
| Titre | Vulnérabilités dans Spring Framework |
| Date de la première version | 13 septembre 2011 |
| Date de la dernière version | – |
| Sources | Bulletins de sécurité Springsource du 09 septembre 2011 |
| 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 à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

Spring Framework versions 2.x et 3.x.

## 3 Résumé

Plusieurs vulnérabilités de Spring Framework ont été corrigées. Certaines permettent l'exécution de code arbitraire à distance.

## 4 Description

Spring Framework permet le développement d'application Java/JEE.

Plusieurs vulnérabilités de Spring Framework ont été corrigées :

- (CVE-2011-2730) une double interprétation d'éléments en langage EL permet à un utilisateur malveillant d'obtenir des informations sans en avoir le droit ;
- (CVE-2011-2731) un problème de concurrence dans *RunAsManager* permet à un utilisateur malveillant d'élever ses privilèges ;
- (CVE-2011-2732) une erreur dans le traitement de connexions et des déconnexions permet à un utilisateur malveillant d'injecter du code dans une réponse HTTP ;
- (CVE-2011-2894) des erreurs dans la *de-serialization* d'objets permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

# 5 Solution

Les versions 2.0.7, 2.5.6.SEC03, 2.5.7.SR02 et 3.0.6 remédient à ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

- Bulletins de sécurité Springsource du 09 septembre 2011 :
  http://www.springsource.com/security/cve-2011-2730
  http://www.springsource.com/security/cve-2011-2731
  http://www.springsource.com/security/cve-2011-2732
  http://www.springsource.com/security/cve-2011-2894
- Référence CVE CVE-2011-2894 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2894
- Référence CVE CVE-2011-2730 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2730
- Référence CVE CVE-2011-2731 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2731
- Référence CVE CVE-2011-2732 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2732
- Référence CVE CVE-2011-2894 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2894

# Gestion détaillée du document

**13 septembre 2011** version initiale.