

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Apache Struts

---

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-2011-AVI-681>

---

### Gestion du document

Référence	CERTA-2011-AVI-681
Titre	Vulnérabilité dans Apache Struts
Date de la première version	13 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apache Struts S2-007
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.

## 2 Systèmes affectés

Apache Struts versions 2.0.0 à 2.2.3.

## 3 Résumé

Une vulnérabilité a été corrigée dans Apache Struts. Cette vulnérabilité peut être utilisée par une personne malintentionnée distante pour injecter et exécuter des expressions OGNL (Object Graph Navigation Language).

## 4 Description

Une vulnérabilité, causée par un mauvais contrôle des données saisies par l'utilisateur, a été corrigée dans Apache Struts. Cette vulnérabilité peut être utilisée par une personne malintentionnée distante pour injecter et exécuter des expressions OGNL (Object Graph Navigation Language).

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Apache Struts S2-007 :  
<http://struts.apache.org/2.x/docs/s2-007.html>

## **Gestion détaillée du document**

**13 décembre 2011** version initiale.