

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Joomla!

---

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-2010-AVI-318>

---

### Gestion du document

Référence	CERTA-2010-AVI-318
Titre	Multiples vulnérabilités dans Joomla!
Date de la première version	19 juillet 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurité Joomla! du 15 juillet 2010
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

Injection de code indirecte à distance.

## 2 Systèmes affectés

*Joomla!* versions 1.5.19 et antérieures.

## 3 Résumé

De multiples vulnérabilités dans *Joomla!* permettent de réaliser des injections de code indirectes.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Joomla!*. Elles permettent à un utilisateur connecté au *back-end* de réaliser des injections de code indirectes. L'une d'entre elles permet d'obtenir des informations sur les chemins internes de *Joomla!*.

## 5 Solution

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

## 6 Documentation

- Bulletins de sécurité Joomla! du 15 juillet 2010 :  
<http://developer.joomla.org/security/news/315-20100701-core-sql-injection-internal-path-exposure.html>  
<http://developer.joomla.org/security/news/316-20100702-core-xss-vulnerabilites-in-back-end.html>  
<http://developer.joomla.org/security/news/317-20100703-core-xss-vulnerabilites-in-back-end.html>  
<http://developer.joomla.org/security/news/318-20100704-core-xss-vulnerabilites-in-back-end.html>

## Gestion détaillée du document

**19 juillet 2010** version initiale.