

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-2009-AVI-263>

---

### Gestion du document

Référence	CERTA-2009-AVI-263
Titre	Multiples vulnérabilités dans Joomla!
Date de la première version	01 juillet 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Joomla! 20090604, 20090605 et 20090606 du 01 juillet 2009
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.

## 2 Systèmes affectés

*Joomla!* versions 1.5.x antérieures à 1.5.12.

## 3 Résumé

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

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Joomla!* :

- la variable HTTP\_REFERER n'est pas correctement traitée, ce qui permet de récupérer des *cookies* (20090604) ;
- la variable PHP\_SELF n'est pas correctement filtrée, ce qui permet d'injecter du code javascript (20090605) ;

- plusieurs fichiers ne vérifient pas si la variable `_JEXEC` a été définie, ce qui provoque l’affichage du chemin d’installation de certains scripts (20090606).

## 5 Solution

Se référer aux bulletins de sécurité de l’éditeur (voir Documentation).

## 6 Documentation

- Bulletins de sécurité Joomla! 20090604 du 01 juillet 2009 :  
<http://developer.joomla.org/security/news/298-20090604-core-frontend-xss-httppreferer-not-properly-filtered.html>
- Bulletins de sécurité Joomla! 20090605 du 01 juillet 2009 :  
<http://developer.joomla.org/security/news/299-20090605-core-frontend-xss-phpself-not-properly-filtered.html>
- Bulletins de sécurité Joomla! 20090606 du 01 juillet 2009 :  
<http://developer.joomla.org/security/news/300-20090606-core-missing-jexec-check.html>

## Gestion détaillée du document

**01 juillet 2009** version initiale.