

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-289>

Gestion du document

Référence	CERTA-2009-AVI-289
Titre	Vulnérabilités dans Joomla!
Date de la première version	24 juillet 2009
Date de la dernière version	–
Source(s)	Annonces de sécurité Joomla! du 22 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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Joomla! 1.5.x.

3 Résumé

Deux vulnérabilités découvertes dans le gestionnaire de contenu Joomla! permettent à un utilisateur distant malintentionné de contourner la politique de sécurité et ainsi porter atteinte à l'intégrité et la confidentialité des données.

4 Description

L'une des vulnérabilités, causée par un manque de vérification sur certains fichiers, permet à une personne malveillante de porter atteinte à la confidentialité des données.

La seconde vulnérabilité, présente dans l'éditeur TinyMCE inclus dans le CMS Joomla!, permet à un individu, non authentifié, de déposer des fichiers arbitraires sur le serveur. Les fichiers ainsi téléchargés peuvent servir à contrôler le système (cf. CERTA-2009-ACT-002 dans la section Documentation).

5 Solution

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

6 Documentation

- Annonces de sécurité Joomla! #301 et #302 du 22 juillet 2009 :
<http://developer.joomla.org/security/news/301-20090722-core-file-upload.html>
<http://developer.joomla.org/security/news/302-20090722-core-missing-jexec-check.html>
- Bulletin d'actualité CERTA-2009-ACT-002 du 09 janvier 2009, «Une compromission discrète» :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-002/CERTA-2009-ACT-002.html>

Gestion détaillée du document

24 juillet 2009 version initiale.