



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 15 novembre 2011
N° CERTA-2011-AVI-640

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-2011-AVI-640>

Gestion du document

Référence	CERTA-2011-AVI-640
Titre	Vulnérabilités dans Joomla!
Date de la première version	15 novembre 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Joomla! du 14 novembre 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

- Accès à distance ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Joomla! versions 1.7.2 et antérieures dans la branche 1.7 et 1.6 ;
- Joomla! versions 1.5.24 et antérieures dans la branche 1.5.

3 Résumé

Deux vulnérabilités dans Joomla! permettent de réaliser une injection de code indirecte à distance et de modifier le mot de passe d'un utilisateur.

4 Description

Deux vulnérabilités ont été découvertes dans Joomla! :

- un mauvais filtrage permet de réaliser une injection de code indirecte dans le *backend* (branches 1.6 et 1.7) ;

- une faiblesse dans la génération de l'aléa lors de la réinitialisation d'un mot de passe permet de le modifier (branches 1.5, 1.6 et 1.7).

5 Solution

Les versions 1.5.25 et 1.7.3 corrigent ces vulnérabilités.

6 Documentation

- Bulletins de sécurité Joomla! du 14 novembre 2011 :
<http://developer.joomla.org/security/news/373-20111101-core-xss-vulnerability>
<http://developer.joomla.org/security/news/374-20111102-core-password-change>
<http://developer.joomla.org/security/news/375-20111103-core-password-change>

Gestion détaillée du document

15 novembre 2011 version initiale.