



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 mars 2011
N° CERTA-2011-AVI-144

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-2011-AVI-144>

Gestion du document

Référence	CERTA-2011-AVI-144
Titre	Multiples vulnérabilités dans Joomla!
Date de la première version	10 mars 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Joomla! du 07 mars 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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

Joomla! versions 1.6.0 et antérieures.

3 Résumé

De multiples vulnérabilités dans *Joomla!* permettent, entre autres, de réaliser des dénis de service à distance et diverses injections.

4 Description

De multiples vulnérabilités ont été découvertes dans *Joomla!*. Celles-ci permettent :

- d’obtenir de l’information sur le système, notamment sur les chemins d’installation ;
- de réaliser diverses injections (XSS et CSRF) ;
- de consommer tout l’espace disque disponible, ce qui provoque un déni de service ;
- de modifier indument des articles (cela nécessite un compte légitime).

5 Solution

Se référer aux bulletins de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation). La version 1.6.1 de *Joomla!* corrige ces vulnérabilités.

6 Documentation

- Bulletins de sécurité Joomla! du 07 mars 2011 :
<http://developer.joomla.org/security/news/328-20110201-core-sql-injection-path-disclosure>
<http://developer.joomla.org/security/news/329-20110202-core-path-disclosure>
<http://developer.joomla.org/security/news/330-20110203-core-xss-vulnerabilities>
<http://developer.joomla.org/security/news/331-20110204-core-xss-vulnerabilities>
<http://developer.joomla.org/security/news/332-20110301-core-information-disclosure>
<http://developer.joomla.org/security/news/333-20110302-core-redirect-vulnerabilities>
<http://developer.joomla.org/security/news/334-20110303-core-information-disclosure>
<http://developer.joomla.org/security/news/335-20110304-core-unauthorised-access>
<http://developer.joomla.org/security/news/336-20110305-core-csrf-vulnerability>
<http://developer.joomla.org/security/news/337-20110306-core-dos-vulnerabilities>
<http://developer.joomla.org/security/news/338-20110307-core-xss-vulnerabilities>
<http://developer.joomla.org/security/news/339-20110308-core-csrf-vulnerability>

Gestion détaillée du document

10 mars 2011 version initiale.