



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2008
N° CERTA-2008-AVI-456-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-2008-AVI-456>

Gestion du document

Référence	CERTA-2008-AVI-456-001
Titre	Vulnérabilités de Joomla!
Date de la première version	11 septembre 2008
Date de la dernière version	19 septembre 2008
Source(s)	Bulletins de sécurité Joomla! du 09 septembre 2008
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.

2 Systèmes affectés

Joomla! version 1.5.6 et versions précédentes.

3 Résumé

Plusieurs vulnérabilités affectent le logiciel Joomla!. Elles permettent de contourner la politique de sécurité ou de porter atteinte à l'intégrité des données.

4 Description

Une vulnérabilité dans JRequest permet de modifier des variables et, par exemple, d'injecter des caractères non désirés.

Un défaut dans le générateur de nombres aléatoires permet de deviner les mots de passe et les jetons créés par l'application.

Deux vulnérabilités permettent l'envoi de pourriel et la redirection vers des sites malveillants.

5 Solution

La version 1.5.7 corrige ces problèmes.

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

6 Documentation

- Site du projet Joomla! :
<http://www.joomla.org>
- Bulletins de sécurité Joomla! du 09 septembre 2008 :
<http://developer.joomla.org/security/news/271-20080901-core-jrequest-variable-injection.html>
<http://developer.joomla.org/security/news/272-20080902-core-random-number-generation-flaw.html>
<http://developer.joomla.org/security/news/273-20080903-core-commailto-spam.html>
<http://developer.joomla.org/security/news/274-20080904-core-redirect-spam.html>
- Référence CVE CVE-2008-4102 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4102>
- Référence CVE CVE-2008-4103 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4103>
- Référence CVE CVE-2008-4104 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4104>
- Référence CVE CVE-2008-4105 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4105>

Gestion détaillée du document

11 septembre 2008 version initiale.

19 septembre 2008 ajout des références CVE.