Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 novembre 2005
N° CERTA-2005-AVI-471

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du logiciel 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-2005-AVI-471

Gestion du document

Référence	CERTA-2005-AVI-471
Titre	Multiples vulnérabilités du logiciel Joomla!
Date de la première version	28 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Joomla! du 21 novembre 2005
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Joomla! version 1.03 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans Joomla! permettent à un utilisateur mal intentionné d'effectuer des attaques par injection de requêtes SQL ou de type *Cross Site Scripting*.

4 Description

Joomla! est un logiciel libre de gestion de contenu (CMS, Content Management System).
Plusieurs vulnérabilités ont été découvertes dans ce logiciel :

– La première vulnérabilité se situe au niveau du module *Polls* et permet d'injecter des requêtes SQL malicieuses à distance;

– La seconde se situe au niveau de la classe *mosDBTable* et permet aussi d'injecter des requêtes SQL malicieuses à distance;
– Enfin, la dernière se situe au niveau de plusieurs scripts, et permet d'effectuer des attaques de type *Cross Site Scripting*.

5 Solution

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

6 Documentation

– Bulletin de sécurité de Joomla! :
http://www.joomla.org/content/view/499/66/
– Référence CVE CVE-2005-3771 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3771
– Référence CVE CVE-2005-3772 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3772
– Référence CVE CVE-2005-3773 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3773

Gestion détaillée du document

28 novembre 2005 version initiale.