Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 février 2008
N° CERTA-2008-ALE-002-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Joomla!

Gestion du document

Référence	CERTA-2008-ALE-002-001
Titre	Vulnérabilité dans Joomla!
Date de la première version	14 janvier 2008
Date de la dernière version	25 février 2008
Source(s)	CERTA
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Toutes les versions de *Joomla!* de la branche 1.0 depuis la version 1.0.11.

3 Résumé

Une vulnérabilité dans *Joomla!* permet d'exécuter du code arbitraire à distance.

4 Description

Un mécanisme dans *Joomla!*, appelé `RG_EMULATION`, permet de contourner le paramétrage de la variable `register_globals` dans le fichier de configuration de `PHP`. Lorsque la variable `RG_EMULATION` est positionnée à `1` dans le fichier `configuration.php` (à la racine de *Joomla!*), il est possible d'exécuter du code arbitraire à distance sur le serveur.

Dans les versions de *Joomla!* antérieures à 1.0.11, la variable `RG_EMULATION` était définie dans le fichier `globals.php`. Une évolution de *Joomla!* d'une version antérieure à 1.0.11 vers la version 1.0.11 ou supérieure entraîne la suppression de la définition de la variable `RG_EMULATION`. Lorsque la variable `RG_EMULATION` n'est pas du tout définie dans le fichier `configuration.php`, celle-ci est positionnée par défaut à `1`, ce qui permet l'exécution de code arbitraire à distance.

5 Contournement provisoire

Il existe plusieurs contournements provisoires :

- dans le fichier `configuration.php`, vérifier que la variable `RG_EMULATION` est positionnée à `0`. Si elle n'est pas définie, ajouter la ligne :
  `$RG_EMULATION = '0';`
- changer le comportement par défaut de *Joomla!* lorsque la variable `RG_EMULATION` n'est pas définie, en remplaçant `1` par `0` dans la ligne 27 du fichier `globals.php` ;
- migrer vers la branche 1.5 de *Joomla!* ou utiliser un autre gestionnaire de contenu.

6 Solution

Mettre à jour en version 1.0.15.

7 Documentation

- Site de *Joomla!* :
  http://www.joomla.org/
- Avis CERTA-2008-AVI-104 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-104/

Gestion détaillée du document

14 janvier 2008 version initiale.
25 février 2008 ajout des sections Solution et Documentation.