Avis de vulnérabilité
Advisory

ISEC-V2012-01-v-1.1

Joomla!
Divulgation d'informations

Notre métier : préserver le vôtre.

WWW.INTRINSEC.COM
215 AV G. CLEMENCEAU 92024 NANTERRE ● TÉL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78
SAS AU CAPITAL DE 480 000 € ● SIREN 402 336 085 ● TVA FR 19 402 336 085 ● APE 721Z

AVIS ISEC-V2012-01-v-1.1

Éditeur : **Joomla!**

Produit : **Joomla!**

Titre : **Divulgation d'informations**

Identifiant Intrinsec : **ISEC-V2012-01-v-1.1**

Date de publication : **2 mars 2012**

Date de dernière mise à jour : **2 mars 2012**

Niveau de risque : **Faible**

Exploitable : **À distance**

Impact :

- Exposition de données sensibles

Niveau de risque de Joomla! : **Faible**

Description :

Un attaquant doit posséder des identifiants utilisateurs valides sur un site Web Joomla! ainsi qu'un accès à l'interface d'administration. À cause d'un problème de filtrage, il peut accéder à certaines fonctionnalités de l'interface d'administration. En particulier, il peut lire :

- Avec Joomla! 1.5.x, la version exacte de Joomla! et des informations concernant la configuration (« Informations système », « Paramètres PHP », « Fichier de configuration » et « Informations PHP »)
- Avec Joomla! 1.7 avant 1.7.4, la version exacte de Joomla!

Versions concernées :

Joomla! 1.5.x, Joomla! 1.6.x et Joomla! 1.7.x avant 1.7.4

Solutions :

Effectuer la mise à jour vers la version 1.7.4, 2.5.0 ou une version plus récente. De plus, restreindre l'accès à l'interface d'administration (n'autoriser que certaines adresses IP) peut être un *workaround*.

Référence :

http://developer.joomla.org/security/news/382-20120101-core-information-disclosure

Crédit :

Vulnérabilité découverte par Erwan Péton (Erwan.Peton@Intrinsec.com)

Vulnérabilité divulguée en concertation avec l'éditeur

Historique :

2012-01-03: Découverte de la vulnérabilité

2012-01-06: Notification de Joomla! Security Strike Team

2012-01-24: Sortie d'une nouvelle version de Joomla! (1.7.4)

ADVISORY ISEC-V2012-01-v-1.1

Editor: **Joomla!**

Product: **Joomla!**

Title: **Information disclosure**

Intrinsec ID: **ISEC-V2012-01-v-1.1**

Publication date: **March 2 2012**

Last update: **March 2 2012**

Risk level: **Low**

Exploitable: **Remotely**

Impact:

- Sensitive data exposure

Joomla! severity: **Low**

Description:

The attacker needs to have valid user credentials to a Joomla! site and access to the administration interface. Due to inadequate filtering, he can access some functionality in the administration interface. Specifically, he can read:

- With Joomla! 1.5.x, exact Joomla! version, data about articles and data about configuration ("System Information", "Relevant PHP Settings", "Configuration File" and "PHP Information")
- With Joomla! 1.7.x before 1.7.4, exact Joomla! version

Versions affected:

Joomla! 1.5.x, Joomla! 1.6.x and Joomla! 1.7.x before 1.7.4

Solution:

Update to Joomla! to 1.7.4, 2.5.0 or higher. Moreover, restrict access to the administration login page (allow only some IP address) can be a workaround.

Reference:

http://developer.joomla.org/security/news/382-20120101-core-information-disclosure

Credits:

Vulnerability discovered by Erwan Péton (Erwan.Peton@Intrinsec.com)

Vulnerability disclosed in coordination with the editor

History:

2012-01-03: Vulnerability discovery

2012-01-06: Joomla! Security Strike Team notification

2012-01-24: New Joomla! version released (1.7.4)