



## CENTRE DE CYBERSÉCURITÉ DU BURKINA FASO

*Notre objectif est de réduire la vulnérabilité du cyberspace, de gérer les incidents de sécurité informatique et de renforcer la culture de cybersécurité*

# ALERTE

## Vulnérabilité de sécurité critique dans Joomla!

### Systèmes affectés

Joomla! versions antérieures à 3.4.6

### Aperçu

Une vulnérabilité a été découverte dans Joomla!. Elle serait massivement exploitée par des pirates depuis quelques jours.

### Description

Il s'agit d'une vulnérabilité de sécurité grave qui peut être facilement exploitée pour exécuter des commandes à distance. Une société spécialisée dans la sécurisation des sites web précise qu'une vague d'attaques provenant des adresses IP 146.0.72.83, 74.3.170.33 et 194.28.174.106 avait débuté avant la mise en ligne du correctif. En plus de ces adresses IP, des marqueurs de détection dans les fichiers de log sont fournis : la présence de la chaîne "JDatabaseDriverMysqli" ou de la chaîne "O:" dans l'entête HTTP User-Agent.

### Impact

La faille concerne une exécution de commande à distance. Si un site Joomla est compromis, les attaquants peuvent introduire du code malveillant sur une page ou rediriger les internautes vers d'autres sites corrompus.

### Solution

Une mise à jour de sécurité est disponible sur le [site officiel de Joomla!](#). Elle contient 4 correctifs à des vulnérabilités de sécurité et inclut également un renforcement du système de réinitialisation du mot de passe.

CIRT-BF recommande aux utilisateurs :

- de faire la mise à jour immédiate vers la version 3.4.6 ;
- de rechercher les occurrences de "JDatabaseDriverMysqli" ou "O" dans le fichier de log ainsi que des connexions

depuis les adresses IP 146.0.72.83, 74.3.170.33 et 194.28.174.106.

## **Références**

- [1] <https://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-vulnerability.html>;
- [2] <http://assistance.apweb.fr/securite-joomla.html>.

## **Révisions**

- Publication Initiale – décembre 14, 2015

[Retour haut de page](#)