Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 1 août 2016
N° CERTFR-2015-ALE-013-001

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Joomla!

Gestion du document

Référence	CERTFR-2015-ALE-013
Titre	Vulnérabilité dans Joomla!
Date de la première version	14 décembre 2015
Date de la dernière version	01 août 2016
Source(s)	Bulletin de sécurité Joomla! du 14 décembre 2015
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(s)

– exécution de code arbitraire à distance

2 - Systèmes affectés

Joomla! versions antérieures à 3.4.6

3 - Résumé

Une vulnérabilité a été découverte dans *Joomla!*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

Une mise à jour de sécurité a été publiée aujourd'hui sur le site officiel de *Joomla!*.

Cependant, une société de sécurité informatique précise qu'une vague d'attaques provenant des adresses IP 146.0.72.83, 74.3.170.33, 93.179.68.167, 199.182.234.132, 185.15.185.17, 37.61.232.173 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.

Le CERT-FR recommande, pour les utilisateurs de *Joomla!*, la mise à jour immédiate vers la version 3.4.6 ainsi que la recherche de la chaîne "JDatabaseDriverMysqli" dans le fichier de log ainsi que des connexions depuis les adresses IP 146.0.72.83, 74.3.170.33, 93.179.68.167, 199.182.234.132, 185.15.185.17, 37.61.232.173 ou 194.28.174.106.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Joomla! du 14 décembre 2015
  https://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-vulnerability.html
- Entrée de blog de la société Sucuri
  https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html

Gestion détaillée du document

14 décembre 2015 version initiale.
18 décembre 2015 mise à jour des adresses IP.
1 août 2016 clôture de l'alerte.