Joomla victime d'une faille zero day exploitée

Si WordPress fait (trop) souvent parler de lui pour les failles de sécurité de ses plug-in et les risques d'infection induits pour les visiteurs des sites qui les exploitent, un autre outil populaire de développement web est aujourd'hui victime d'une vulnérabilité infectieuse : Joomla. Le système de gestion de contenus web, également massivement utilisé par les développeurs, a alerté l'existence d'une vulnérabilité zero day *« qui peut être facilement exploités »*, annonce la firme de sécurité Sucuri. *« Si vous utilisez Joomla, vous devez mettre à jour [le correctif] immédiatement »*, poursuit-elle dans sa page de blog.

Deux jours d'exploitation

Toutes les versions de Joomla, de la 1.5 à la 3.4.5, sont concernées par la faille. Ce qui inquiète particulièrement Sucuri, c'est que *« cette vulnérabilité est déjà exploitée dans les faits et l'a été au cours des 2 derniers jours »*. Découverte le 12 décembre, et annoncée le 13, la brèche n'a été comblée que le 14. Son exploitation permet l'exécution de code à distance.

Sur ses installations, Sucuri a repéré plusieurs exploitations de la faille, d'abord depuis une seule adresse IP le 12 décembre, puis deux autres le lendemain. Le 14 *« la vague d'attaques est encore plus grande, affectant tous nos site et pots de miel*, indique la société de sécurité. *Cela signifie que probablement d'autres sites Joomla sont aussi ciblés. »*

Injection de code malveillant

La faille implique la chaîne « User-Agent » du navigateur qui permet de s'identifier en tant que client auprès du serveur. Les attaquants peuvent ainsi *« effectuer une injection d'objet via l'agent HTTP de l'utilisateur qui ouvre l'exécution d'une commande à distance »*. Un site infecté pourrait permettre à l'assaillant d'injecter du code malveillant sur une page ou rediriger un visiteur vers un autre site.

Souhaitons que les administrateurs de sites Joomla corrigent au plus vite le bug. Le CMS Open Source est notamment utilisé par des entreprises comme Citibank, Honda, Peugeot, l'université de Harvard ou des administrations.

Lire également
La politique biaisée de divulgation des zero day de la NSA
Bingo : 1 million de dollars pour une faille zero day dans iOS 9
Des failles zero day trouvées chez Kaspersky et FireEye