Une faille dans PHPMailer fragilise des CMS et des millions de sites web

Un chercheur polonais en sécurité, Dawid Golunski, a trouvé une faille critique dans PHPMailer. Ce script PHP donne aux développeurs la capacité d'automatiser l'envoi de mail. Cette librairie est très connue et des millions de sites web l'utilisent, ainsi que les CMS les plus populaires comme WordPress, Joomla, Drupal, SugarCRM, vTiger CRM, Mantis, XOOPS, Zikula, etc.

Concrètement, cette faille ouvre la voie à des attaques capables de « *cibler des composants classiques d'un site web tels que les formulaires de contact ou d'inscription, la réinitialisation d'un mot de passe et d'autres qui envoient des e-mails à l'aide d'une version vulnérable de la classe PHPMailer* », indique le spécialiste.

La vulnérabilité a été référencée sous le code CVE-2016-10033 et vise les versions antérieures à la 5.2.18. Cette dernière corrige la faille et a été publiée le jour de Noël. Étant donné la période, la mise à jour sur l'ensemble des sites va prendre du temps et parfois elle ne sera jamais appliquée. Pour les éditeurs de CMS, WordPress et Drupal préparent des correctifs de sécurité mettant à jour la librairie.

Les cybercriminels plus rapides

Sur une page, le chercheur donne quelques indications sur le *modus operandi* de la vulnérabilité. Il précise avoir élaboré un prototype fonctionnel d'une attaque pour démontrer la véracité de sa découverte. Il reste cependant volontairement laconique dans ses explications pour donner du temps aux webmasters et aux éditeurs de corriger leurs versions de PHPMailer embarqué dans leur code.

Mais malgré sa prudence, des pirates ont analysé les différences entre le code source de la version non corrigée et celui de la version corrigée. Les cybercriminels ont mené des travaux de rétro-ingénierie sur la mise à jour de sécurité afin d'identifier la faille. Pour *in fine*, diffuser leur propre code d'attaque disponible sur GitHub et ExploitDB.

A lire aussi :

PHP au top des langages à la source de failles

Salaires : des disparités entre développeurs PHP en 2016

crédit photo © ra2studio – shutterstock