WordPress encore faillible via des plugins utilisant Genericons

Pas une semaine sans que WordPress ne soit victime d'une nouvelle attaque ? Quelques jours après les risques d'attaques par cross-site scripting (XSS) via les commentaires, la version 4.2 (et précédentes) de la plate-forme de publication de sites web est de nouveau victime d'une faille l'exposant à une autre agression XSS. Une brèche de sécurité découverte par la firme de sécurité Sucuri.

Cette fois, c'est le paquet Genericons d'icones vectorisées en polices qui est affecté. La vulnérabilité se concentre plus précisément sur le fichier « example.html » qui accompagne le *package*. *« La vulnérabilité XSS est très simple à exploiter et se déploie au niveau du Document Object Model (DOM) »*, indique David Dede de Sucuri. Les attaques XSS qui s'appuient sur l'API DOM sont difficilement repérables car elles s'exécutent au sein du navigateur sans effectuer de requêtes au serveur ce qui les rendent invisibles aux pare-feux et d'autant plus difficile à bloquer, précise l'expert en sécurité. Pour s'exécuter, elles nécessitent néanmoins d'amener l'utilisateur à cliquer sur un lien infectieux afin de modifier le DOM. Mais une fois cette étape passée, l'attaque XSS permet d'exécuter du code javascript au sein du navigateur pour, potentiellement, prendre la main sur le site pour peu que la victime dispose de droits d'administration.

Des attaques en cours

Selon Sucuri, deux plug-ins qui exploitent Genericons par défaut sont d'ores et déjà affectés : JetPack, un outil d'optimisation et gestion de la performance qui compte plus d'un million d'activations, et le thème TwentyFifteen installé par défaut depuis WordPress 4.1 fourni en décembre 2014. *« Le nombre exact est difficile à évaluer, mais le plugin et le thème sont présents par défaut sur des millions d'installations WordPress »*, ajoute le responsable en sécurité à l'origine de la découverte de la vulnérabilité. Une faille visiblement déjà exploitée alors que des rapports d'attaques commençaient à remonter au prestataire avant la mise à jour de la plate-forme.

Car WordPress s'est évidemment empressé de corriger cette nouvelle brèche de sécurité. La version 4.2.2 supprime simplement le fichier « example.html » et ajoute un mécanisme de vérification de la présence de ce document non indispensable dans le répertoire wp-content pour l'effacer au besoin. La nouvelle version du célèbre CMS utilisé par 23% des sites web (selon l'éditeur) en profite pour corriger 13 autres bugs (dont on trouvera la liste sur cette page). Il va sans dire que la mise à jour s'impose le plus rapidement possible ou, au moins, la suppression du fichier problématique.

Lire également
WordPress : une nouvelle faille critique se loge dans les commentaires
Alertes aux attaques par défacement de sites WordPress
La faille Ghost dans Linux s'étend à PHP et WordPress

crédit photo © drx – Fotolia.com