La faille Ghost dans Linux s'étend à PHP et WordPress

La semaine dernière, Qualys levait le voile sur une vulnérabilité touchant la **glibc**, la bibliothèque C de base des systèmes Linux. Elle s'appuyait notamment sur l'appel des fonctions gethostbyname () et gethostbyname2 (). La vulnérabilité Ghost permet de prendre le contrôle d'un système à distance, sans même connaître ses identifiants administrateur. La plupart des OS Linux étaient touchés : Centos, RHEL, Fedora 5, 6, et 7 Ubuntu 12.04. Les spécialistes de Qualys ont élaboré un prototype d'attaque exploitant la vulnérabilité dans le serveur de mail Exim et ont inclus dans la liste des victimes, Apache, Sendmail, Nginx, MySQL, CUPS, Samba, etc.

Des chercheurs de la firme de sécurité, Sucuri, ont **élargi la liste des solutions potentiellement vulnérables**. « *Nous avons de bonnes raisons de croire que **les applications PHP** pourraient également être affectées par la fonction gethostname () wrapper* » explique dans un blog Marc-Alexandre Montpas. Il poursuit son raisonnement en parlant d'un exemple où cela peut poser problème « *dans **WordPress** qui utilise une fonction wp_http_validate _url() pour valider chaque notification de lien URL* ». Cette fonction s'appuie sur gethostbyname (). Un attaquant pourrait alors passer par ce vecteur pour insérer une URL malveillante et ainsi déclencher un débordement de la mémoire tampon côté serveur et obtenir une élévation de privilège.

Selon nos confrères d'Ars Technica, il existe peu de preuves montrant une exploitation effective de la faille Ghost contre les serveurs de messagerie ou des sites web. Cependant, les chercheurs appellent à la vigilance et à mettre à jour dès que possible les systèmes Linux.

A lire aussi :

Après SSL 3.0, la faille Poodle s'étend à TLS
Des serveurs Linux enrôlés sur les botnets IptabLes et IptabLex