HTTPoxy, une faille vieille de 15 ans se réveille

Vieilles bases de données volées et vieux malware réarrangés, la mode est au vintage dans le domaine de la cybersécurité. Un développeur de Vend (logiciel pour la distribution), Dominic Scheirlinck, a déniché une faille datant de 2001 et qui refait surface, nommée HTTPoxy. Découverte en 2001 par Randal L. Schwartz, cette vulnérabilité touche le module libwww-perl qui a du mal à gérer les en-têtes de HTTP_Proxy. Elle a essaimé ensuite sur curl (avril 2001), sur Ruby (juillet 2012), Nginx (novembre 2013) et maintenant sur PHP, Python et Go dans les environnements CGI.

Le problème est que les applications web CGI recevant des requêtes PHP entrantes vident le contenu des en-têtes Proxy dans la variable d'environnement HTTP_Proxy sans nettoyage. Or cette variable est utilisée dans de nombreuses applications pour configurer automatiquement un client local de proxy sortant. Quand un utilisateur effectue une autre requête PHP, elle s'appuie sur le proxy configuré localement pour atteindre la destination demandée.

Un attaquant peut se servir de cette faille pour infecter les serveurs et forcer une application CGI à utiliser un proxy malveillant pour ses requêtes HTTP sortantes. Un cas typique d'attaque de l'homme du milieu (MiTM).

Une atténuation facile à mettre en œuvre

Dominic Scheirlinck explique que cette vulnérabilité peut être facilement atténuée. Par contre, les mesures d'atténuation « doivent être intégrées le plus tôt et le plus en amont possible. Il faut aller à la périphérie du réseau, là où les requêtes HTTP entrent dans le système. De cette façon vous pourrez colmater beaucoup de logiciels vulnérables à la fois », explique le développeur. Il recommande également de nettoyer complètement l'en-tête Proxy soit via un proxy reverse, soit via le firewall qui nettoie l'en-tête Proxy.

Reste que plusieurs applications et projets Open Source sont vulnérables à HTTPoxy en mode CGI. Le CMS Drupal a mis à jour ses versions 8.x pour atténuer ce type d'attaques dans la librairie Guzzle PHP. Découverte en février dernier, Dominic Scheirlinck a laissé le temps aux éditeurs de corriger cette faille. Plusieurs d'entre eux ont publié des conseils, comme US CERT, Apache, Red Hat, Nginx, CloudFlare et Akamai.

A lire aussi :

PHP au top des langages à la source de failles

Les salaires des développeurs PHP en hausse en 2015

crédit photo © Nata-Lia – shutterstock