NTPsec remet les pendules d'Internet à l'heure de la sécurité

Il y a quelques semaines nous vous faisions part des différents failles trouvées dans le protocole NTP. Ce dernier participe à la synchronisation des horloges d'Internet. Des chercheurs ont trouvé des moyens pour dérégler ce grand horloger du web dans le but de mener des attaques de type de DDoS (avec un phénomène d'amplification connu depuis 2014), des interceptions de communications chiffrées et même du sabotage.

Le problème est que NTP (Network Time Protocol) est incontournable et inchangeable dans l'organisation de l'Internet aujourd'hui. Des transactions financières à la sauvegarde des dossiers, ce protocole maintient les serveurs et les PC à l'heure. Au même titre qu'OpenSSL visé dans l'affaire Heartbleed, NTP n'a pas bénéficié pendant plusieurs années de développement et de maintenance. Seule une personne s'en occupait et encore à temps partiel.

NTPSec 0.9 en piste

Heureusement NTP a bénéficié de l'aide de l'Initiative Core Infrastructure à la fois pour sécuriser le protocole, mais aussi financer son successeur **NTPSec**. Ce dernier est toujours en travaux, mais Eric S Raymond, spécialiste reconnu de l'Open Source et en pointe sur ce projet, a annoncé sur son blog la sortie en beta de NTPSec 0.9. Il insiste bien sur le caractère expérimental. « *C'est une version initiale qui a quelques défauts en raison du remplacement traumatique (mais nécessaire) de l'autoconf du système.* »

Cependant, il indique toujours à l'attention des développeurs, que « *la fonction essentielle, c'est-à-dire la synchronisation de l'horloge via NTP est solide. Utiliser la version 0.9 en production peut-être jugé comme aventureux, mais pas complétement fou* ». Sur la sécurité de NTPSec, le gourou glisse que « *les principaux changements sont profonds et non visibles pour les utilisateurs. Mais la plus grande évolution est que le code a été très sérieusement sécurisé, pas uniquement par des corrections de vulnérabilités, mais par des mesures internes préventives pour bloquer plusieurs failles* ».

Un toilettage en profondeur pour NTP

Dans le même temps, il participe aussi à la sécurisation du NTP actuel. Il a obtenu le soutien du Center for Trustworthy Scientific Cyberinfrastructure et le Center for Applied Cybersecurity Research de l'Université de l'Indiana. Et des avancées ont été constatées avancent nos confrères de *ZDnet*. Le référentiel propriétaire de NTP a migré vers un dépôt Git accessible au public. Le code a été toiletté pour le moderniser et le simplifier pour obtenir une version plus stable. Résultat, les spécialistes ont réduit les lignes de code de NTP de 31 000 à 884. Enfin, une documentation appropriée à l'attention des nouveaux développeurs a été créée. Les travaux sont donc en bonne voie et vont se poursuivre.

A lire aussi :

Failles NTP : la machine à détraquer le temps menace aussi le chiffrement
Heartbleed : un an après, la faille est tombée dans l'oubli

Crédit Photo : Rangizz-Shutterstock