OpenSSL encore touché par des failles de sécurité

Après Heartbleed, la librairie Open Source de chiffrement OpenSSL est sous haute surveillance, notamment de la Core Infrastructure Initiative qui a mis récemment en place un audit sur cette bibliothèque. Et même le groupe en charge d'OpenSSL s'est penché sur sa création et vient d'annoncer la découverte de 7 vulnérabilités.

Deux de ces failles sont considérées comme critiques. Selon le cabinet de sécurité Lexsi. La première *« permet une **exécution de code à distance** sur des applications aussi bien serveur que client instrumentant la couche de chiffrement du protocole UDP OpenSSL DTLS (Datagram Transport Layer Security) »*. Il ajoute que *« ce protocole étant majoritairement présent dans des applications offrant des fonctionnalités de visioconférence, il est probable que les acteurs majeurs tels que Cisco seront impactés et qu'ils nous livreront les correctifs adéquats sous peu »*.

La deuxième vulnérabilité critique a été découverte par Masashi Kikuchi. Elle permet une **attaque de type « man-in-the-middle »** rendant possible le déchiffrement et la modification du trafic, explique Lexsi. Mais cette faille a une particularité : **elle est présente dans le code d'OpenSSL depuis 15 ans**, c'est-à-dire décembre 1998, soit depuis le début du projet Open Source. Masashi Kikuchi souligne que ce bug aurait pu être réparé depuis longtemps en testant le code d'OpenSSL.

Une loi des séries sur le chiffrement Open Source

Les autres failles sont considérées comme moins importantes, avec des risques de déni de service ou injection de code. Le groupe OpenSSL a indiqué que l'ensemble de ces bugs a été corrigé et demande aux utilisateurs de mettre à jour les versions de la librairie.

La semaine dernière un chercheur portugais avait découvert une méthode baptisée Cupidon qui injecte la faille Heartbleed dans les routeurs WiFi, mais aussi dans les smartphones Android. OpenSSL n'est pas le seul projet Open Source à connaître des problèmes de sécurité. Cette semaine, un chercheur de la société ayant découvert Heartbleed a trouvé une faille dans la bibliothèque de chiffrement GnuTLS. Un correctif a aussitôt été publié pour les différentes distributions Linux qui utilisent ce service.

A lire aussi :

Faille Heartbleed : la check-list pour s'en sortir