Freak affaiblit le chiffrement des navigateurs Apple et Android

Une équipe de chercheurs en sécurité, dont une majorité de Français de l'INRIA (Karthik Bhargavan, Antoine Delignat-Lavaud, Benjamin Beurdouche et Jean Karim Zinzindohoué) et de Microsoft, ont découvert une faille qui impacte les navigateurs des terminaux Apple et Android. Cette vulnérabilité nommée FREAK (Factoring attack on RSA-EXPORT Keys), enregistré sous le code **CVE 2015-0204, est vieille de 10 ans** et provient d'une ancienne politique du gouvernement américain qui interdisait l'exportation de solution de chiffrement fort. En substitut, les autorités américaines livraient aux pays étrangers des services de chiffrement plus faibles logo-typés « **export grade** ».

Un cadavre dans SSL/TLS

Cette interdiction a été levée à la fin des années 90, mais ce chiffrement faible a été intégré dans des protocoles largement utilisés dans le monde entier y compris aux Etats-Unis. Bill Brenner, spécialiste de la sécurité chez Akamai, souligne dans un blog que « *cette politique américaine a eu des conséquences sur le protocole SSL/TLS de deux façons. La première était d'ajouter des suites de chiffrements qui reposaient sur des clés courtes et facilement cassables. Elles sont toutes identifiables par le suffixe EXP* ».

Il ajoute que la « *seconde orientation est plus problématique et comme le disent les puristes, c'est même très laid. Lorsqu'un client se connecte à un serveur, il chiffre la communication (appelé liaison SSL) en utilisant la clé RSA du serveur. Dans la configuration d'exportation (export grade),* ***cette clé était de 512 bits****. A l'époque, cela pouvait être qualifiée de chiffrement fort. Aujourd'hui, pour 100 dollars en utilisant les ressources du Cloud, cette clé peut être cassée en moins d'une demi-journée* ».

Une attaque de type homme du milieu

La suite de la découverte est présentée par Matthew Green, professeur en cryptographie qui a aidé le groupe de chercheurs. « *La faille a été trouvée dans les clients Open SSL (utilisé par les navigateurs sous Android) et dans les clients TLS/SSL (utilisés par Safari d'Apple). Elle permet des attaques de type « homme du milieu » pour dégrader la sécurisation de la connexion de « strong RSA » à « export grade » RSA* ». Il confie que « *ces attaques sont réelles et exploitables contre un grand nombre de sites web y compris des sites gouvernementaux* ». Les chercheurs ont par exemple fait un test avec la page web de la NSA. Avec succès (cf les captures d'écran ci-dessous).

Dans des démonstrations vidéo, ils montrent que plusieurs sites sont vulnérables à ce type d'attaque (IBM, Symantec), notamment ceux qui utilisent le système d'authentification ou le bouton Like de Facebook via Facebook JavaScript SDK. Ils ont pu ainsi accéder sans difficultés aux comptes sur des sites comme wepay.com, kickstarter ou dashlane (gestionnaire de mot de passe qui a corrigé ses serveurs en conséquence). Interpellé, Facebook a depuis corrigé son programme connect.facebook.net.

Navigateurs pour Android et Apple touchés

Dans un entretien au *Wahsington Post*, un des chercheurs souligne que « *sur 14 millions de sites web dans le monde qui proposent du chiffrement, environ 5 millions restent vulnérables encore ce matin* ». La raison de cette baisse de sites fragiles provient **d'une mise à jour des serveurs d'Akamai**, largement utilisé par les sites en tant que fournisseur CDN. Dans le détail, **le navigateur Chrome pour desktop ne semble pas concerné** par cette vulnérabilité. Par contre, l**a version sous Android** est exposée tout comme **Safari d'Apple**. La firme de Cupertino a indiqué aux journalistes du *Post* qu'elle travaillait sur un correctif à la fois pour MacOS X et pour iOS.

Cette affaire montre à la fois la faiblesse du suivi de la politique américaine en matière de sécurité et de chiffrement en particulier. Un oubli intentionnel pour favoriser la surveillance des agences de renseignement ou simple défaut gratuit et sans arrière-pensée ? Elle s'attaque aussi encore une fois à des questions de protocoles de communications chiffrées. L'année 2014 avait connu l'affaire Heartbleed qui avait secoué le monde de l'Open Source et celui des entreprises et qui touchait également Open SSL. D'autres failles dans SSL comme Poodle ont été mises à jour plus récemment, obligeant les acteurs du web à prendre des mesures pour déconnecter certains protocoles trop anciens et donc vulnérables.

A lire aussi :

Nogofail : Google traque les failles de SSL et TLS
5 questions pour comprendre le déchiffrement SSL

Crédit Photo : SergeyNivens-Shutterstock