Après Heartbleed et Shellshock : une faille touche SSL 3.0

Trois chercheurs de Google viennent de découvrir un bogue dans SSL 3.0, **protocole de chiffrement très employé par les navigateurs et sites Web**. Dévoilée dans une note de recherche publiée par le projet OpenSSL, la librairie de chiffrement Open Source très largement employée sur le Web, la vulnérabilité en question peut permettre à un assaillant de **dérober les cookies d'un navigateur**. « *C'est assez complexe. L'assaillant doit bénéficier d'une position privilégiée dans le réseau* », a expliqué **Ivan Ristic**, un expert en SSL de la société Qualys, à nos confrères de Reuters. L'exploitation de la faille passe par une attaque de type « man-in-the-middle », l'attaquant devant s'interposer entre le site Web et le navigateur ciblé.

SSL 3.0 : « à éviter complètement »

Si le problème n'a donc pas la gravité de ceux créés par les failles Heartbleed (un problème d'implémentation dans OpenSSL) ou ShellShock (une faille dans l'interpréteur de lignes de commandes Unix Bash), il en partage une caractéristique : la **très large diffusion de la technologie concernée**. Si SSL 3 .0 a été supplanté par TLS (Transport Layer Security) 1.0, puis 1.1 et 1.2, la plupart des implémentations conserve une compatibilité avec SSL 3.0 afin de continuer à fonctionner sans heurt avec les bases installées. Conséquence : quand un client et un serveur ne parviennent pas à établir une connexion dans un protocole plus récent, **ils basculent sous SSL 3.0 et son cryptage RC4 datant de… 1987**. C'est ce mécanisme appelé 'downgrade dance' que les chercheurs de Google exploitent pour mener leur attaque baptisée Poodle (Padding oracle on downgraded legacy encryption).

Une solution immédiate consiste à désactiver SSL 3.0. « *Pour assurer un chiffrement fiable, SSL 3.0 doit être évité complètement* », écrivent les chercheurs de Google. Le désactiver est envisageable sur les navigateurs. Faute de quoi un serveur malicieux, pensé pour mener des attaques ciblant cette vulnérabilité, pourrait pousser les clients à établir une connexion sous SSL 3.0, en refusant l'initiation d'un échange via TLS. Reste que **désactiver ce protocole** va générer un grand nombre d'incompatibilités, notamment avec les systèmes historiques.

crédit photo : nasirkhan / shutterstock

A lire aussi :
5 questions sur la faille Shell Shock visant Bash
Faille Heartbleed : la check-list pour s'en sortir