Chiffrement : tous les navigateurs vont abandonner l'algorithme RC4

Les trois principaux éditeurs de navigateurs, Google, Microsoft et Mozilla, sont au moins d'accord sur un point : l'algorithme de chiffrement RC4 est dépassé. Les trois concurrents ont annoncé le 1er septembre que leurs navigateurs respectifs (Chrome, Edge, Internet Explorer et Firefox) ne supporteraient plus la technologie vieillissante à partir de l'année prochaine.

Conçu en 1987 par Ronald Rivest, l'un des inventeurs de l'algorithme à clef publique RSA, RC4 est un générateur de bits pseudo-aléatoires, à clef secrète, considéré aujourd'hui comme insuffisamment sécurisé par les experts en cryptographie. Problème : il est toujours largement utilisé dans des protocoles comme WEP, WPA et surtout TLS, qui sécurise les échanges sur Internet, notamment en transformant HTTP en HTTPS.

Suivre les recommandations de l'IETF

En février, l'Internet Engineering Task Force (IETF) recommandait de ne plus exploiter RC4 pour les échanges TLS. L'organisme, qui produit la plupart des standards Internet, notait alors qu'une des faiblesses du protocole, dévoilée en 2013, mettait en danger les communications par TLS, la faille étant exploitable avec des capacités de calcul accessibles. Les éditeurs de navigateur ont alors pris de premières mesures, limitant l'usage de RC4 aux serveurs ne proposant pas d'autres options lors de la phase de négociations entre serveur et client qui précède l'établissement d'une connexion sécurisée.

Google, Microsoft et Mozilla franchissent donc aujourd'hui un pas supplémentaire en proscrivant définitivement l'algorithme vieillissant. Ce sera le cas pour Chrome « *en janvier ou février 2016* ». Même échéance pour Microsoft avec Edge – le navigateur de Windows 10 – et IE pour Windows 7, 8.1 et 10. Mozilla est plus précis, et va stopper le support de RC4 sur la version 44 de Firefox, attendue le 26 janvier. Le trafic sécurisé par RC4 est d'ores et déjà très faible. Selon Google, seulement 0,13 % des connexions HTTPS au sein de Chrome (parmi les utilisateurs ayant accepté la collecte de ces statistiques) utilisent encore l'algorithme de 1987.

A lire aussi :

Le chiffrement source de multiples failles de sécurité

Emmanuel Thomé, Inria : « Les clefs de chiffrement de 768 bits ne suffisent plus »

LogJam : nouvelle faille dans le chiffrement des sites Web

Crédit photo : Maksim Kabakou / Shutterstock