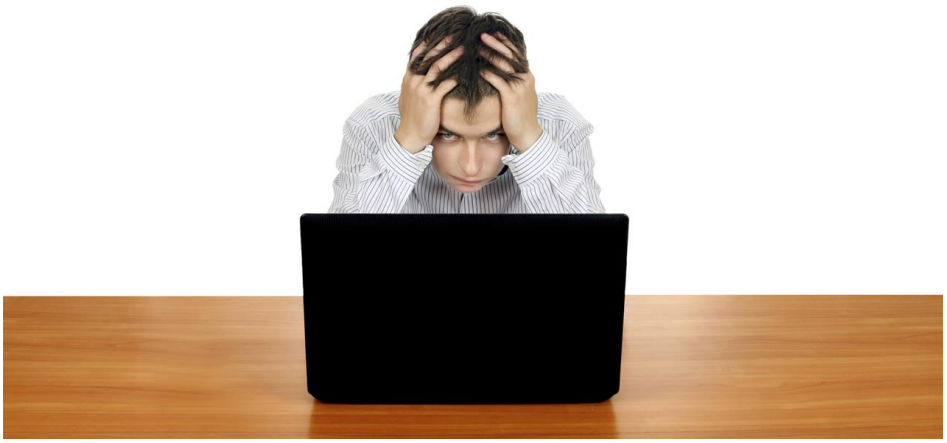
Après FREAK, une nouvelle faille dans le chiffrement des connexions

	Après FREAK, une nouvelle faille dans le chiffrement des connexions

Une nouvelle faille de sécurité vient de remonter à la surface : #Logjam. Né des cendres de FREAK, elle reprend le même principe de fonctionnement et permet d'établir une connexion chiffrée avec une clé trop petite pour être réellement efficace.

Au début du mois de mars, la #faille FREAK secouait Internet, pour plusieurs raisons. Tout d'abord, car elle permettait (et permet toujours) d'intercepter des échanges de données chiffrés entre un serveur et un navigateur. Ensuite car il s'agissait d'un reliquat des années 90 lorsque les États-Unis limitaient l'exportation des systèmes de chiffrements à 512 bits maximum (voir cette actualité pour plus de détail). Bien évidemment, bon nombre de serveurs et de navigateurs avaient été rapidement mis à jour suite à cette découverte.

Il convient néanmoins de relativiser puisqu'il faut procéder à une attaque de type « homme du milieu » pour l'exploiter, et donc être sur le même réseau (un « hot-spot » Wi-Fi par exemple), ce qui n'est pas toujours des plus pratiques. On est loin de la portée de Heartbleed par exemple, qui permettait à n'importe qui de lire des données directement dans la mémoire d'un serveur (identifiant, mot de passe, carte bancaire, etc.).

De FREAK à Logjam, toujours la même histoire de chiffrement « faible »

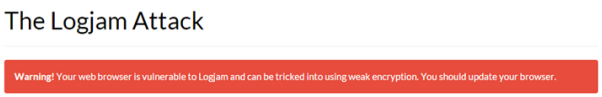
Mais une faille peut en cacher une autre et voilà désormais qu'il est question de Logjam. Elle est détaillée dans ce document, signé par des chercheurs de l'INRIA de Paris et de Nancy, de l'université de Pennsylvanie, de Johns Hopkins, du Michigan et de chez Microsoft Research. Selon les chercheurs, « *cette attaque rappelle FREAK, mais elle est due à une faille dans le protocole TLS plutôt qu'à une vulnérabilité dans son implémentation, et elle cible un échange de clés Diffie-Hellman plutôt que d'un échange de clés RSA* ».

Avec la faille FREAK et l'utilisation de la fonction « export RSA », un serveur répond avec une clé RSA de 512 bits, tandis qu'avec Logjam et « DHE_EXPORT », serveur et navigateur procèdent à un échange de clés via le protocole Diffie-Hellman, mais dans des groupes de 512 bits seulement… ce qui n'est pas suffisant pour résister à une attaque. On notera que ce problème avait déjà été évoqué par certains il y a plusieurs mois. La situation n'est donc pas nouvelle, mais elle prend une autre tournure.

Serveurs et navigateurs doivent se mettre à jour

Là encore, le problème concerne les navigateurs et les serveurs : il suffit que l'un des deux n'accepte pas un groupe de 512 bits pour que l'attaque échoue. De plus, et comme avec FREAK, il faut être sur le même réseau pour que cela fonctionne via une attaque de l'homme du milieu, ce qui limite évidemment la portée, mais n'enlève rien à sa dangerosité.

Du côté des navigateurs, Internet Explorer ne semble pas vulnérable si l'on en croit l'outil de test proposé par le site WeakDH.org, mais Chrome et Firefox le sont. Adam Langley, un cryptanalyste qui travaille chez Google, s'est exprimé sur le sujet sur l'un des forums du géant du web : « *En se basant sur leur travail, nous avons désactivé TLS False-Start avec Diffie-Hellman dans Chrome 42, qui est la version stable depuis plusieurs semaines maintenant* [NDLR : on est passé à Chrome 43 depuis ce matin, mais cela ne change rien sur le principe]*. Cette attaque sur les serveurs vulnérables sera un peu plus difficile* ».



Passer à 1 024 bits minimum, voire mieux à Diffie-Hellman sur des courbes elliptiques

Pour autant, cela n'est pas encore suffisant et Adam Langley ajoute que « *le tronc commun du code de Chrome changera afin d'imposer une nouvelle taille de 1024 bits pour Diffie-Hellman. Même si cela entraînera des problèmes pour certains sites, le travail d'aujourd'hui montre que nous ne devrions pas considérer de tels sites comme sécurisés de toute manière* ». Il précise que « *ce changement est en bonne voie d'être inclus dans Chrome 45* », mais que le calendrier pourrait être plus rapide.

Mais tout cela ne sera probablement qu'une solution temporaire. En effet, les chercheurs à l'origine de la publication de Logjam indiquent qu'un groupe de 1 024 bits peut être « cassé » par un pays ayant suffisamment de moyens (on pense notamment à la NSA qui décrypte à tout-va), et cela ne fera qu'empirer avec le temps. Le cryptographe de Google rejoint cette conclusion : « *Un minimum de 1024 bits ne suffit pas sur le long terme. Malheureusement, parce que certains clients ne prennent pas en charge les groupes de DH supérieurs à 1024 bits, et parce que TLS ne négocie pas spécifiquement certains groupes, il serait très problématique de pousser cette limite au-dessus de 1024. Alors que nous approchons de l'élimination du chiffrement RSA sur 1024 bits, nous nous interrogeons de manière plus générale sur la prise en charge des groupes non elliptiques DHE dans TLS* ». Cela laisse entendre que cette méthode pourrait disparaitre à terme, en tout cas chez Google.

Il existe en effet une version plus sécurisée de ce protocole : ECDHE pour Elliptic curve Diffie–Hellman (ou bien encore Diffie-Hellman sur des courbes elliptiques). Pour Google, « *les serveurs qui utilisent actuellement DHE devraient se mettre à jour et passer à ECDHE. Si cela est impossible, utilisez au moins DHE avec des groupes de 1024 bits et ne soyez pas trop surpris si Chrome commence à utiliser du chiffrement RSA avec votre site dans le futur* ».

Un guide des bonnes pratiques et un site pour tester navigateurs et serveurs

Cette recommandation est d'ailleurs également faite par l'équipe de chercheurs qui a mis en ligne un petit guide du déploiement de Diffie-Hellman, ainsi qu'un outil de test. Il recommande de désactiver les fonctions Export Cipher Suites, déployer un système de Diffie-Hellman sur des courbes elliptiques et utiliser un groupe fort et unique pour chaque serveur.

Comme toujours, on devrait voir arriver une série de correctifs dans les prochaines semaines, à la fois côté navigateur et serveur. Cela ne devrait pas tarder puisque les principaux concernés ont été mis au courant avant que la faille ne soit rendue publique.

Réagissez à cet article

Source : *Logjam : après FREAK, une nouvelle faille dans le chiffrement des connexions – Next INpact*