LogJam : nouvelle faille dans le chiffrement des sites Web

Une nouvelle faille de sécurité affecte les connexions chiffrées entre un serveur Web ou d'e-mail et un utilisateur. La vulnérabilité, baptisée LogJam, toucherait **8,4 % du million de sites Web HTTPS les plus populaires dans le monde**, ainsi qu'un grand nombre de serveurs de messagerie (environ 15 % des serveurs SMTPS). La faille a été découverte par des chercheurs issus de l'Inria, de Microsoft Research et des universités américaines John Hopkins, du Michigan et de Pennsylvanie. Dans le détail, elle concerne **tous les protocoles reposant sur SSL ou son successeur TLS** (Transport Layer Security), comme HTTPS, SSH ou encore SMTPS. Elle est présente au sein de SSL depuis environ deux décennies et le successeur de ce protocole de sécurisation – TLS – en a logiquement hérité.

Protocol	Vulnerable to Logjam
HTTPS — Top 1 Million Domains	8.4%
HTTPS — Browser Trusted Sites	3.4%
SMTP+StartTLS — IPv4 Address Space	14.8%
POP3S — IPv4 Address Space	8.9%
IMAPS — IPv4 Address Space	8.4%

La découverte de LogJam découle en réalité de celle de Freak (Factoring attack on RSA-Export Keys), mise au jour en mars. Cette famille de failles trouve son origine dans la législation américaine, qui, pendant de longues années, a limité la taille des clefs à 512 bits sur les logiciels destinées à l'export, afin d'empêcher un chiffrement fort des communications.

Si ces restrictions ont aujourd'hui disparu, LogJam exploite toutefois les particularités techniques héritées de cette réglementation. L'exploitation de la faille, qui se loge dans des algorithmes appelés Diffie-Hellman facilitant l'échange de clefs préalable à la sécurisation d'une connexion (tandis que Freak se niche dans l'échange de clefs RSA), consiste à **tromper un serveur Web ou d'e-mail** pour lui faire à croire que son correspondant emploie une **longueur de clef limitée**. Le poussant à établir une communication mal protégée, qui peut alors être déchiffrée en quelques minutes. Pour mener à bien cette attaque de type Man-in-the-middle, un hacker doit toutefois se trouver sur le même réseau que sa victime.

Mises à jour des navigateurs

Les entreprises qui ont mis à jour leurs logiciels pour combler la faille Freak sont d'ores et déjà protégées, les rustines empêchant les logiciels de chiffrement de recourir aux protocoles les plus friables, ceux conçus pour se plier aux restrictions à l'export des autorités américaines. Cette mise à niveau n'a toutefois pas touché les navigateurs, qui n'ont pas été patchés après Freak, leur concepteur ne voulant pas se couper de la petite minorité de sites exploitant encore des clefs de

512 bits. Mais LogJam va changer la donne : Microsoft a déjà mis à jour Internet Explorer ; Firefox et Safari doivent suivre. **La situation est plus complexe du côté des serveurs d'e-mail**, la plupart d'entre eux étant peu mis à jour.

Les chercheurs à l'origine de la découverte de la faille ont publié un guide de déploiement de l'algorithme Diffie-Hellman pour les éditeurs de solutions et conseillent de recourir uniquement aux clefs de 2048 bits (le 768 et le 1024 bits étant vulnérables à des attaques menées par des Etats, estiment ces spécialistes). Les développeurs et sysadmin sont eux invités à mettre leurs librairies TLS à jour et à rejeter l'initiation de communications cryptées avec des clefs inférieures à 1024 bits.

A lire aussi :

Une application Android sur 10 victime de Freak
5 questions pour comprendre le déchiffrement SSL

Crédit photo : Maksim Kabakou / Shutterstock