http://www.lemondeinformatique.fr/actualites/lire-freak-une-faille-critique-qui-menace-le-chiffrement-web-60435.html

LEMONDE INFORMATIQUE

Le 04 Mars 2015

Freak, une faille critique qui menace le chiffrement web

La faille Freak permet à des attaquants de dégrader la sécurité des connexions web en passant d'un chiffrement fort à un mode de chiffrement faible initialement intégré à des logiciels destinés à l'export. (Crédit : D.R.)

La vulnérabilité Freak qui touche SSL et TLS affecte de nombreux sites populaires, ainsi que l'OS Android, le navigateur Safari et les applications utilisant une version d'Open SSL antérieure à 1.0.1k.

Une autre faille de sécurité vient d'être découverte dans le protocole SSL (Secure Sockets Layer) et son successeur, TLS (Transport Layer Security). Baptisée Freak (pour Factoring attack on RSA-EXPORT Keys), elle permet à un attaquant d'intercepter du flux chiffré circulant entre postes clients et serveurs. Elle permet en effet de forcer les navigateurs à utiliser un chiffrement sur 512 bits en lieu et place du 2048 bits. La faille touche de nombreux sites très fréquentés et différents logiciels, comme l'OS mobile Android de Google ou le navigateur Safari d'Apple. Les applications qui utilisent une version d'OpenSSL antérieure à 1.0.1k sont également vulnérables, selon le bulletin d'alerte publié sur le site CVE. Cette faille existe apparemment depuis plusieurs années.

Des mises à jour pour iOS et OS X seront livrées la semaine prochaine, a indiqué Apple. De son côté, Google a indiqué avoir fourni des correctifs à ses partenaires pour protéger les connexions Android vers les sites vulnérables.

Un problème qui prend sa source dans les années 90

Le problème vient de restrictions imposées par le gouvernement américain au début des années 1990. Dans un billet, Ed Felten, professeur d'informatique à l'Université de Princeton, rappelle qu'elles empêchaient les éditeurs de logiciels d'exporter des produits intégrant du chiffrement fort. Certains fournisseurs ont donc commercialisé en dehors des Etats-Unis une version de leurs produits comportant des clés de chiffrement faible. Lorsque la loi a changé, la fonctionnalité destinée au mode export n'a pas été supprimée du protocole car certains logiciels s'y référaient encore, explique Ed Felten.

La faille Freak permet ainsi aux attaquants de dégrader la sécurité des connexions en passant au mode de chiffrement faible initialement intégré à des logiciels destinés à l'export. Les serveurs et postes clients vulnérables sont ceux qui acceptent les suites cipher RSA_EXPORT. Les sites web qui y recourent risquent de voir leurs connexions HTTPS interceptées. Le site freakattack.com fournit une liste des principaux sites qui doivent arrêter de les supporter.

Article de Maryse Gros avec IDG News Service