Une faille de sécurité dans TCP permet de pirater la plupart des sites Web

Selon une étude de chercheurs américains, l'implémentation d'un standard relativement récent d'Internet (RFC 5961) dans Linux expose les communications TCP – un des protocoles centraux du Net – à des risques. Un assaillant pouvant interrompre une connexion ou injecter des contenus ou des portions de code malveillant dans ladite communication. Lors de la conférence Usenix, qui se tient en ce moment à Austin (Texas), les chercheurs de l'Université de Californie et du laboratoire de recherche de l'armée américaine ont fait la démonstration des dangers de la technique qu'ils ont mis sur pied, en injectant du code Javascript malveillant dans une page légitime du quotidien américain *USA Today*. Cette exploitation de la faille qu'ils ont mise au jour, et qui permettrait par exemple à un attaquant de récupérer les login et mot de passe des utilisateurs via un formulaire de son crû injecté dans une page légitime, n'est possible qu'avec des sites recourant à des communications non chiffrées (le HTTP simple donc). Pour les sites recourant au HTTPS, l'attaque 'se limite' à interrompre la connexion.

Linux seulement, mais cela suffit

Selon les chercheurs, qui parlent d'une technique « *efficace et fiable* » qu'ils ont pu tester largement, il faut compter environ une minute pour pirater une communication entre un serveur et un utilisateur, et y injecter des contenus malveillants. Et il suffit qu'une des extrémités de la communication soit exposée à la faille pour que l'attaque soit possible. Un détail qui décuple les risques découlant de la découverte de Yue Cao, Zhiyun Qian, Zhongjie Wang, Tuan Dao, Srikanth V. Krishnamurthy et Lisa Marvel, les chercheurs à l'origine de l'étude. En effet, l'implémentation de RFC 5961 se limite pour l'instant à Linux – OS où il est présent depuis 2012 – et n'a pas encore été déployé sur Windows ni OS X. Or une très large majorité des serveurs Web sont basés précisément sur l'OS Open Source.

Si les développeurs en charge du noyau Linux ont livrés un patch pour cette faille (CVE-2016-5696), avec la version 4.7 mise en ligne il y a environ trois semaines, celle-ci n'a pas encore été intégrée par les principaux éditeurs de distributions. Paradoxalement, l'empressement des développeurs Linux à intégrer les derniers standards de sécurité – car la RFC 5961 était supposée la renforcer – se retourne ici contre eux…

Nul besoin d'infecter le serveur

Dans leur étude, les chercheurs expliquent que la faille résulte de changements dans la façon dont TCP initie une connexion. « *Notre attaque est basée sur une technique permettant à un assaillant off-path (donc non présent sur le 'trajet' de la communication, NDLR) de déterminer efficacement la séquence de nombres employée dans une connexion TCP tant par le client que par le serveur* », écrivent-ils.

Si des attaques de même nature (dites off-path) existent depuis des années, l'introduction de RFC 5961 rend leur exploitation bien plus efficace. Car, selon les chercheurs, un assaillant potentiel a

seulement besoin de disposer d'une connexion Internet pour tester si deux machines sur le réseau communiquent entre elles par une ou plusieurs connexions TCP et pour les pirater. Nul besoin de monitorer ou de contrôler le trafic comme avec les attaques de type Man-in-the-Middle. « *Nous insistons sur le fait que cette attaque peut être menée sans déployer aucun code malicieux ni sur le serveur, ni sur le client* », notent les chercheurs. Selon l'un d'entre eux, Zhiyun Qian, interrogé par nos confrères d'*Ars Technica*, la faille découle d'un « *problème subtil* » et provient tant du standard RFC lui-même que de son implémentation. « *Le RFC est écrit de telle façon que si les OS l'implémentent de but en blanc, ce sera problématique* », avertit Zhiyun Qian.

Eliminer les nœuds légitimes de Tor

Dans leur étude, les chercheurs soulignent encore les conséquences que cette faille peut avoir pour Tor. Des assaillants pourraient en effet exploiter la vulnérabilité pour faire tomber des communications sur le réseau d'anonymisation, par exemple celles reliant un utilisateur final à un point d'entrée, un point d'entrée à un relais ou un relais à un point de sortie. Rappelons que l'attaque qu'ils décrivent permet de mettre fin à toute communication TCP, fut-elle chiffrée. Fermer des points de sortie légitimes de Tor s'avère très dangereux pour ce réseau, car cela augmente les risques de voir la connexion détournée vers un nœud malicieux, contrôlé par l'assaillant. « *La règle par défaut dans Tor est que si une connexion tombe entre deux nœuds, par exemple entre un relais et un point de sortie, le relais va chercher un nouveau point de sortie pour établir une nouvelle connexion*, détaillent les chercheurs. *Si un assaillant peut choisir les connexions qui vont tomber, alors il peut potentiellement imposer l'utilisation de certains points de sortie.* »

A lire aussi :

Comment le Machine Learning aide à débusquer les failles de sécurité

Scan de ports TCP : comment la NSA et le GCHQ préparent leurs attaques

Failles NTP : la machine à détraquer le temps menace aussi le chiffrement

Crédit photo : GlebStock / Shutterstock