Redirection de ports : quand les VPN révèlent leurs secrets

Les protocoles VPN souffrent d'une erreur de design qui rend possible **l'identification de l'adresse IP de leurs utilisateurs**. C'est en tout cas ce qu'affirme le fournisseur de VPN Perfect Privacy, qui a mis au jour cette vulnérabilité qu'il a baptisée « port fail » (l'échec de port). Selon cette société, cette faiblesse touche les fournisseurs offrant des services de redirection de port (sauf à avoir pris des mesures particulières). Tant sur IPSec (Internet Protocol security) que sur PPTP (point-to-point tunnelling protocol). Les clients VPN basés sur OpenVPN sont aussi concernés.

5 des 9 principaux fournisseurs

Pour mettre en œuvre le mécanisme décrit par Perfect Privacy, un assaillant doit d'abord disposer d'un compte chez le même fournisseur que sa cible et avoir activé la redirection de port. Il doit ensuite récupérer l'adresse IP de sortie de sa victime, en la poussant à consulter un site qu'il contrôle ou en la récupérant par un autre biais (IRC, torrent). « *Nous avons testé cette méthode avec neuf fournisseurs importants de VPN offrant la redirection de port. Cinq d'entre eux étaient vulnérables à l'attaque ; ils ont été informés de cette faille en amont afin de pouvoir la corriger avant cette publication*, écrit Perfect Privacy dans un billet de blog. *Cependant, d'autres fournisseurs de VPN peuvent être encore vulnérables à cette attaque comme nous n'avons pas pu tous les tester.* » Private Internet Access a ainsi comblé cette faille et a versé 5 000 dollars à son concurrent pour récompenser ses efforts de recherche.

Pour Perfect Privacy, **les utilisateurs de BitTorrent** sont particulièrement menacés, car s'ils utilisent la redirection de port par défaut sur leur logiciel client, un assaillant n'aura même pas besoin de leur faire visiter un site sous son emprise pour récupérer leur IP.

A lire aussi :

Comment la NSA a (probablement) cassé le chiffrement par VPN

Le service web Cisco VPN victime de backdoor

Les VPN commerciaux sont-ils vraiment sécurisés ?

crédit photo © Pavel Ignatov – shutterstock