Les solutions VPN touchées par une faille sur la redirection de ports

Les solutions VPN touchées par une faille sur la redirection de ports

---

Suivre
nVpn.net @nVpnNet
Fixed a possibility to exploit a VPNs PF feature revealing a user’s real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy
01:07 – 27 Nov 2015
4 4 Retweets 2 2 j’aime

La société de sécurité Perfect Privacy a averti hier dans un billet de blog que bon nombre de solutions VPN étaient vulnérables à des attaques par redirection de port. De fait, un grand nombre d'utilisateurs pourraient voir leurs adresses IP réelles être dévoilées par des pirates utilisant les mêmes réseaux.

Les VPN, ou réseaux privés virtuels, sont conçus pour permettre laccès à des ordinateurs distants. Ils sont également souvent utilisés pour masquer les adresses IP dorigine. Mais il n'est finalement pas très compliqué d'obtenir quand même cette information, surtout quand les solutions existantes autorisent la redirection de port et qu'elles ne sont protégées contre des attaques utilisant cette fonctionnalité.

La faille « #VPN Fail »

Hier, la société Perfect Privacy a averti qu'un grand nombre de solutions VPN pouvaient révéler ces adresses IP si un pirate savait où chercher.

Pour que l'attaque fonctionne, il doit se trouver sur le même réseau virtuel que sa victime et connaître son adresse IP de sortie.

Comme l'indique The Hacker News, cette étape est assez simple puisqu'il suffit d'attirer l'utilisateur sur un site évidemment contrôlé par le pirate. Si la redirection de port est activée, le pirate pourra obtenir l'adresse IP réelle de la victime en l'amenant à ouvrir par exemple une image. À partir de là, il devient possible de rediriger le trafic vers un port là encore contrôlé par le pirate, d'où le nom de l'attaque.

Cette faille de sécurité, nommée « VPN Fail » par Perfect Privacy, a donné lieu à un avertissement lancé à de nombreux éditeurs. La plupart sont donc informés et le tir a été corrigé pour des solutions comme Private Internet Access, Ovpn.to et nVPN. Ce dernier est pour le moment le seul à avoir confirmé officiellement que cétait le cas, comme en atteste le tweet ci-dessous.

Perfect Privacy indique cependant que toutes les solutions n'ont pas été testées et que le nombre de produits vulnérables est donc sans doute important.

Clients VPN, systèmes dexploitation, BitTorrentLa faille pose évidemment un vrai problème de sécurité et de vie privée. Les VPN sont très utilisés dans les pays par exemple où la censure est importante, notamment parce qu'ils bloquent le repérage de la géolocalisation.

En conséquence, une faille qui laisserait apparaître la véritable adresse IP ne peut que briser tout l'intérêt de ces solutions et on peut espérer que des correctifs seront rapidement déployés.

La dangerosité de la faille est grande selon Perfect Privacy, puisqu'à cause de la nature même de la faille, on risque de la retrouver dans un très nombre de produits, dont les systèmes d'exploitation.

Elle peut également être utilisée pour piéger des internautes qui se serviraient de BitTorrent. La technique s'exploite d'ailleurs plus rapidement puisque le pirate n'a pas besoin d'amener l'utilisateur sur un site. Il doit simplement se trouver sur le même VPN et avoir activé la redirection de port.

nVpn.net @nVpnNet

Fixed a possibility to exploit a VPNs PF feature revealing a user's real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy

01:07 – 27 Nov 2015

4 4 Retweets 2 2 j'aime

Rien à faire pour linstant du côté de lutilisateur

Dans tous les cas, la victime n'a pas besoin d'avoir l'option activée, et il n'y a donc rien qu'elle puisse faire de son côté. Tous les protocoles liés au VPN, comme OpenVPN et IPSec, sont également concernés. La seule solution est actuellement d'attendre, jusqu'à recevoir une notification de son fournisseur de solution VPN, si bien entendu ce dernier prend la peine de communiquer.

Réagissez à cet article

Source : http://www.nextinpact.com/news/97495-vpn-fail-solutions-vpn-touchees-par-faille-sur-redirection-ports.htm