Plusieurs trous de sécurité pour OpenVPN

OpenVPN, un logiciel libre permettant de créer des réseaux privés virtuels, est toujours confronté à des problèmes de sécurité. Même si Google est prêt à payer des développeurs pour en améliorer la sécurité et que des audits de sécurité ont déjà été menés, les faiblesses persistent. Un chercheur indépendant, Guido Vranken, a analysé le logiciel et a découvert 4 vulnérabilités importantes. Il vient de publier le fruit de ses travaux sur son blog.

La faille la plus critique, la CVE-2017-7521, se situe dans une extension (extract_x509_extension()) qui opère des certificats SSL. Cette brèche peut soit provoquer le blocage du service, via un certificat compromis, soit permettre à un attaquant d'exécuter du code à distance côté serveur via une corruption de mémoire. Guido Vranken ne sait pas si cette vulnérabilité a déjà été utilisée de manière publique, mais, pour peu que des assaillants y aient consacré des efforts et des moyens, l'hypothèse n'est pas exclue. Du côté d'OpenVPN, on accueille cette faille avec retenue : « *le bug ne peut être déclenché que dans des configurations utilisant l'option –x509-alt-username avec une extension x509* ». Or, selon l'équipe d'OpenVPN, cette configuration serait très peu utilisée.

D'autres bugs importants à corriger

Le second bug, CVE-2017-7520, vise la façon dont OpenVPN se connecte à un proxy Windows NTLM version 2. Une attaque de type homme du milieu entre le client et le serveur proxy pourrait soit bloquer le client, soit subtiliser le mot de passe du proxy via une corruption de mémoire.

Enfin, Guido Vranken a découvert deux possibilités de bloquer à distance le serveur. Les bugs CVE-2017-7508 et CVE-2017-7522 peuvent être déclenchés en envoyant des paquets IPv6 malformés ou en envoyant des données tronquées après le processus d'authentification.

Le chercheur en profite pour régler ses comptes avec l'architecture d'OpenVPN, qui n'est pas propice aux tests aléatoires de sécurité (fuzzing). Il cite notamment comme barrière l'exécution de « *programmes externes comme IPconfig et route pour modifier l'état du réseau du système. Ceci est inacceptable dans un environnement de fuzzing* ». Malgré ces coups de griffes, OpenVPN a pris en compte les recherches de Vranken et conseille de mettre à jour les versions 2.4.3 et 2.3.17, premières à bénéficier d'un patch.

A lire aussi :

Redirection de ports : quand les VPN révèlent leurs secrets

Sécurité : 85 % des VPN SSL sont des passoires

Photo credit: tanakawho via VisualHunt.com / CC BY-NC