Attaques DDoS via Memcached : le protocole UDP pointé du doigt

Des milliers de sites internet sont à la merci d'une faille dans le système open source Memcached utilisé dans certains serveurs pour la mise en cache de mémoire distribuée.

Celle-ci peut être utilisée par des hackers pour lancer des attaques massives par déni de service (DDoS) sur les serveurs.

OVH et GitHub en ont déjà fait les frais.

Ce sont plusieurs sociétés de sécurité qui ont découvert le pot aux roses. CloudFlare, fournisseur CDN (Content Delivery Network), a aussi découvert la faille et l'ampleur de la menace.

C'est le port UDP 11211 (UDP pour User Datagram Protocol, est un protocole utilisé par Internet) qui peut être à l'origine d'un trafic entrant de 260 Gb/s. Il a même été reporté des attaques pouvant générer 1,3 Tb/s de trafic.

Généralement Memcached permet d'augmenter les performances des sites Web dynamiques qui utilisent des bases de données pour stocker du contenu. Celui-ci qui est le plus fréquemment accédé est stocké dans de la mémoire cache, afin de réduire les requêtes aux bases de données nécessaires à la diffusion de pages Web. Or, il se trouve que le protocole UDP ne présente aucun contrôle ou système d'authentification.

Selon CloudFlare, l'attaque dite par réflexion est initiée par un serveur usurpant l'adresse IP de la cible et envoyant un paquet de requête de 15 octets. Le serveur non protégé exploitant Memcached lui répond alors avec une quantité de données dans une fourchette comprise entre 134 Ko et 750 ko.

On parle là d'un facteur d'amplification du trafic pouvant ainsi atteindre 51 200.

Tant et si bien que Cloudflare a baptisé cette faille « Memcrashed ».

Si Cloudflare a découvert 5729 serveurs pouvant être ciblés comme sources de trafic DDoS amplifié depuis la découverte de la faille, le moteur de recherche de vulnérabilité Shodan signale au moins 88 000 serveurs Memcached accessibles au public qui pourraient être utilisés comme vecteurs de telles attaques DDoS amplifiées.

Pour limiter la casse, les administrateurs de systèmes disposant de serveurs Memcached sont invités à désactiver complètement la prise en charge d'UDP, ou bien à limiter son accès au minimum en « écoutant » toutes les adresses IP. Il est également fortement conseillé d'utiliser un pare-feu pour empêcher que Memcached ne soit accessible publiquement.

L'usage d'UPD n'est donc pas forcément recommandé. Le cas échéant, un mécanisme vérifiant que le serveur répond systématiquement à une requête avec une taille de paquet strictement inférieure à la demande permet d'éviter de telles attaques DDoS.

(Crédit photo © Google / Connie Zhou)