Issued 3/1/18

Popular Cache Utility Exploited for Massive DoS Attacks

Former Internet Systems Consortium CEO and now Akamai principal architect Barry Raveendran Greene has detailed the reflected DOS attack on his blog and explained it can make it look like the incoming traffic comes from a service provider's router. The attack abuses the memcached distributed in-memory caching utility, used to speed up dynamic Web applications by sharing around the database load. SANS' Johannes Ulrich wrote: “Apparently people are exposing memcached to the internet. For many other services, I would qualify that statement: 'without access control'. But for memcached there is no access control. This is by design.” The mechanism attackers have used was to send memcached instances a request for statistics over UDP, apparently coming from the spoofed victim's IP address. The stats request is 15 bytes long, but the reply is between 1,500 bytes up to hundreds of kilobytes. Qrator Labs reckons its seen attacks reach 500 Gbps. If you're under attack, there are two things to do: block all traffic from port 11211, and if you can, get help from your ISP to block the traffic. Operators are being asked to help block the attacks as well. A note to Australian Network Operators' Group (AUSNOG) suggests implementing Exploitable Port Filters as per these instructions. And if you're a sysadmin whose memcached server is outside the firewall, get it inside, configure it so it doesn't listen on UDP.