To: William H. Flathead III

From: Claudio Facchinetti

Subject: Security issue: TCP SYN Flood DoS

Date: October 18, 2021

The objective of this memo is bring to your attention a potential security issue that could affect any of the company webservers.
With our team we managed to replicate the structure of our deployment on a testbed and analyzed the effects of a TCP SYN flood attack on the client experience.
In case you do not know, a TCP SYN flooding attack is a particular DoS (Denial of Service) attack in which a malicous entity starts send SYN packets to the server so that it fills up the memory allocating structures to handle a connection that will never be concluded.
The detailed results are available in the `graph.xlsx` file, but I would like to comment a little to better explain the situation. In the first case scenario the result is complete disaster: as soon as the attack begins the client is no longer able to get responses in a reasonable time. This is due to the fact that the server is not using the SYN cookies mechanism to delay the creation of the memory structure needed to handle the connection. In this particular case, indeed, the server is really slow to response but is also slow to receive packets, because the router cannot handle such a large amounts of packets.
The situation is better when the SYN cookies are enabled: in this specific case the response times are definitely higher then normal, but connections do complete in a reasonable amount of time. The problems, in this case, seem to be both the router which is overloaded and also the fact that the attacker is spoofing the ip address of the client, however we have no control on the latter.
Just for a matter of completion we tried to disable spoofing and now the client is able to successfully get responses with almost no additional waiting time, exception made for some isolated cases. Those cases could be again due to the fact that the router is overloaded.
This latter hypothesis is confirmed by our final experiment: we tried to eliminate the route and create peer-to-peer connections between the server and both the attacker and the client machines. With this setup the client was slightly affected by the attack, but the difference is almost not noticeable by a human user.
As a precaution I would reccomend to enable SYN cookies on all our webservers and also to setup some kind of load balancing, so that we can be more resilient to DoS attacks, especially distributed ones. As a preventive countermeasure it would be advisable to put into place a firewall/IPS which could impose a rate limit on the requests: this would block naive DoS but would not be effective against spoofing, since the IP would change.