F5 Friday: Mitigating the THC SSL DoS Threat

Lori MacVittie, 2011-28-10

The THC #SSL #DoS tool exploits the rapid resource consumption nature of the handshake required to establish a secure session using SSL.

A new attack tool was announced this week and continues to follow in the footsteps of resource exhaustion as a means to achieve a DoS against target sites.

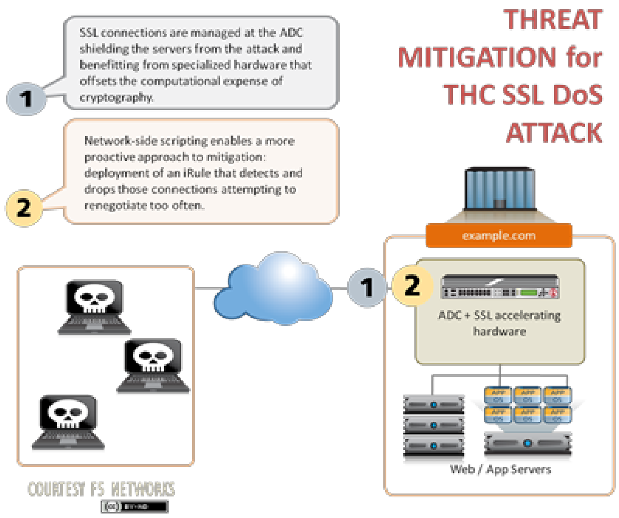
Recent trends in attacks show an increasing interest in maximizing effect while minimizing effort. This means a move away from traditional denial of service attacks that focus on overwhelming sites with traffic and toward attacks that focus on rapidly consuming resources, instead. Both have the same ultimate goal: overwhelming infrastructure, whether server or router or **<**insert infrastructure component of choice**>**.

The latest SSL-based attack falls into the modern category of denial of service attacks in that it's not an attempt to overwhelm with traffic, but rather to consume resources on servers such that capacity and the ability to respond to legitimate requests is eliminated.

The blog post announcing the exploit tools explains:

> Establishing a secure SSL connection requires 15x more processing power on the server than on the client.
>
> THC-SSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet.
>
> This problem affects all SSL implementations today. The vendors are aware of this problem since 2003 and the topic has been widely discussed.
>
> This attack further exploits the SSL secure Renegotiation feature to trigger thousands of renegotiations via single TCP connection.
>
> -- THC SSL DOS Tool Released

As the blog points out, there is no resolution to this exploit. Common mitigation techniques include the use of an SSL accelerator, i.e. a reverse-proxy capable device with specialized hardware designed to improve the processing capability of SSL and associated cryptographic functions. Modern application delivery controllers like BIG-IP include such hardware by default and make use of its performance and capacity-enhancing abilities to offset the operational costs of supporting SSL-secured communication.


THREAT MITIGATION for THC SSL DoS ATTACK
1
SSL connections are managed at the ADC shielding the servers from the attack and benefitting from specialized hardware that offsets the computational expense of cryptography.
2
Network-side scripting enables a more proactive approach to mitigation: deployment of an iRule that detects and drops those connections attempting to renegotiate too often.
example.com
1
2
ADC + SSL accelerating hardware
Web / App Servers
COURTESY F5 NETWORKS

BIG-IP MITIGATION

There are actually several ways in which BIG-IP can mitigate the potential impact of this kind of attack. First and foremost is simply its higher capacity for connections and processing of SSL / RSA operations. BIG-IP can manage myriad more connections – secure or not – than a typical web server and thus it may be, depending on the hardware platform on which BIG-IP is deployed, that the mitigation rests merely on having a BIG-IP in the path of the attack.

In the case that it is not, or if organizations desire a more proactive approach to mitigation, there are two additional options:

1. SSL renegotiation, which is in part the basis for the attack (it's what allows a relatively few clients to force the server to consume more and more resources), can be disabled in BIG-IP v11 and v10.2.3. This may break some applications and/or clients so this option may want to be left as a "last resort" or the risks carefully weighed before deploying such a configuration.

2. An iRule that drops connections over which a client attempts to renegotiate more than five times in a given 60-second interval can be deployed. As noted by David Holmes and the iRule author, Jason Rahm, "By silently dropping the client connection, the iRule causes the attack tool to stall for long periods of time, fully negating the attack. There should be no false-positives dropped, either, as there are very few valid use cases for renegotiating more than once a minute."

The full details and code for the iRule can be found in the DevCentral article "SSL Renegotiation DOS attack – an iRule Countermeasure"

UPDATE 11/1/2011: David Holmes has included an optimized version of the iRule in his latest blog, "The SSL Renegotation Attack is Back." His version uses the normal flow key (instead of a random key), adds a log message, and optimizes memory consumption.

Regardless of the mitigating technique used, BIG-IP can provide the operational security necessary to prevent such consumption-leeching attacks from negatively impacting applications by defeating the attack before it reaches application infrastructure.

Stay safe!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com