Mea Culpa of Death

David Holmes, 2011-28-12

I took a little heat for the last blog post (UDP Packet of Death). Let me explain myself.

I chose the title "UDP Packet of Death" because the vulnerability reminded me of the old Windows 95 "ping of death" vulnerability that had such a great name. But this vulnerability isn't quite as fragile as that ancient one.

The key differentiator for VU#951982 is that it requires a very large number of packets (instead of just one). When a non-matching packet hits the network stack on a non-listening port, normally an ICMP response packet (connection refused) is sent back to the client. When a ***storm*** of non-matching packets hits, most operating systems including Windows and TMOS, will ***throttle*** their ICMP responses because when a system gets hit with 1 million bad packets, it doesn't really help the situation to send out 1 million error responses.

It appears that it is in the throttling code where the vulnerability occurred, according to this write-up by the Microsoft Security Research & Defense group. Here's an excerpt from that page.

> **Vulnerability**
> The vulnerability presents itself in the specific scenario where an attacker can send a large number of specially crafted UDP packets to a random port that does not have a service listening. While processing these network packets it is observed that some used structures are referenced but not dereferenced properly. This unbalanced reference counting could eventually lead to an integer overflow of the reference counter.

Microsoft has since patched the vulnerability, and there are no known exploits in the wild that we've heard of.

I didn't think that this needed to be pointed out, but perhaps it does: of course, any run-of-the-mill firewall (Juniper, Checkpoint, or Fortinet), properly configured, will filter out attacks like this. The point of my blog post was this:

Do you know what ***else*** will filter out this attack? A BIG-IP Local Traffic Manager (LTM).

I talk to a lot of customers that use BIG-IP LTM as a firewall, because it ***works*** and these customers save enormous amounts of money on firewalls that wouldn't even have the same (awesome) performance characteristics as BIG-IP. FYI, Lori MacVittie has a compelling article showing how BIG-IP LTM can be a better firewall than what you might have now.

I don't mind admitting when I could have done a more complete job either in coding or writing.

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