

RE: [fw-wiz] CERT vulnerability note VU# 539363

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-10/0888.html>

From: Stephen Gill (gillsr@yahoo.com)

Date: 10/16/02

From: "Stephen Gill" <gillsr@yahoo.com>

To: "'Paul D. Robertson'" <proberts@patriot.net>, "'Mikael Olsson'" <mikael.olsson@clavister.com>

Date: Wed Oct 16 10:26:02 2002

The essence of the problem is that new flows won't be established. Not allowing new traffic has the unfortunate side effect of not allowing the good and the bad. This affects traffic in any direction for which there has not been an established flow. Let's see... outbound anything (DNS/ICMP/WEB), inbound anything (VPN connections/Hosting services).

] Public-talking hosts should be protectable with simple non-stateful packet

] filtering rules- *especially* those which allow the untrusted side to] initiate connections.

I couldn't agree more. Disable state when you don't need it.

Unfortunately it's not always an option on firewalls but hopefully others will add it.

-- steve

-----Original Message-----

From: proberts@gargoyle.users.patriot.net

[<mailto:proberts@gargoyle.users.patriot.net>] On Behalf Of Paul D. Robertson

Sent: Wednesday, October 16, 2002 8:36 AM

To: Mikael Olsson

Cc: Stephen Gill; firewall-wizards@honor.icsalabs.com

Subject: Re: [fw-wiz] CERT vulnerability note VU# 539363

On Wed, 16 Oct 2002, Mikael Olsson wrote:

> *Although this is something that people need to keep in mind when*
> *picking / designing a firewall, I'd argue that anything north of*
> *a stateless packet filter is going to be vulnerable to these sort*
> *of attacks.*

So will anything south of a firewall- hosts aren't immune to flooding attacks either, with or without state, nor are routers...

> *If you keep state, you will be vulnerable to state table overflows.*

I don't know that "overflow" is the right word here, "exhaustion" seems more fitting.

When I first looked at this, I kind of shrugged and said "So what?" the firewall is doing its job— stopping packets when there's an attack—

The issue is more of how easy that is, than the fact that you can do it. So the real message here is know the failure mode and capacity limits of

the firewalls you use.

If you're being attacked, the firewall not allowing new traffic is probably not a bad thing. For most folks, the ability to create a new state table entry is an "outbound traffic only" issue for firewalls that

aren't "protecting" external services like Web servers.

If you're hosting public resources behind the same firewall that's protecting everything else in your enterprise, you've probably made a questionable architectural decision. If you're keeping state on say inbound SMTP traffic, the question is "Why?" If the 'Net as a whole can

connect to something, the state itself isn't going to do much good. If you're trying to rewrite sequence numbers because of a host that talks to

the public with high predictability, again you're probably made a questionable architectural decision.

Public-talking hosts should be protectable with simple non-stateful packet

filtering rules— *especially* those which allow the untrusted side to initiate connections.

> *Period. The only real question is: how much work does the attacker
> need to put in before it becomes painful for the networks that the
> firewall is protecting? Is being able to resist a 1 Mbps stream
> (~4500 pps) "Not vulnerable"? Is being able resist a 34 Mbps stream
> (~150 kpps) "Not vulnerable"? Or should every single firewall
> vendor report in and say "Vulnerable", and describe what the limit is?*

That's also a scale thing— if a firewall is in front of 10 hosts, the effort to protect them from floods might be scalable to 10x, but if it's

1000 hosts, the amount of protection is almost certainly going to be less than 1000x[1].

> *And, yes, ALG-only firewalls can also be overloaded. It's just a
> different type of 'state'.*

Anything without some sort of artificial rate limiting can be DoS'ed.

What this really says to me is "Don't keep state on stuff that doesn't *need* it." Possibly combined with "if you have a large number of untrused users, make sure your policies let you disconnect them if they cause trouble, and have enough diagnostic infrastructure to be able to figure out where an internal attacker is (personally, I prefer losts of routers.)"

As far as ALG state goes, at least the ALG is the final determination point for the traffic, so it can deal with many issues (such as the CRC one detailed in the vulnerability note) immediately, rather than having to rely on a network reply from a host, or in some cases, just not knowing.

Paul

[1] There are products which scale higher, but they tend to be the kinds

of things you put in front of DSLAMs and cost several hundred thousand dollars each.

Paul D. Robertson "My statements in this message are personal opinions proberts@patriot.net which may have no basis whatsoever in fact." probertson@trusecure.com Director of Risk Assessment TruSecure Corporation