

## RE: [fw-wiz] pixen abnormalities;

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-08/0091.html>

---

**From:** Wes Noonan ([mailinglists\\_at\\_wjnconsulting.com](mailto:mailinglists_at_wjnconsulting.com))

**Date:** 08/26/03

To: "'Melson, Paul'" <PMelson@sequoianet.com>, "'\"R. DuFresne\"" <dufresne@sysinfo.com>' " <IMCEAN  
Date: Tue, 26 Aug 2003 16:19:45 -0500

New one to me too. Sounds like a bogus position they have to me. I'd love to hear of an actually exploit along the lines of what they seem to be worried about.

Wes

> -----Original Message-----

> From: [firewall-wizards-admin@honor.icsalabs.com](mailto:firewall-wizards-admin@honor.icsalabs.com)

[[mailto:firewall-wizards-](mailto:firewall-wizards-admin@honor.icsalabs.com)

> [admin@honor.icsalabs.com](mailto:admin@honor.icsalabs.com)] On Behalf Of Melson, Paul

> Sent: Thursday, August 21, 2003 15:41

> To: "R. DuFresne" <[dufresne@sysinfo.com](mailto:dufresne@sysinfo.com)>; [firewall-](mailto:firewall-wizards@honor.icsalabs.com)

> [wizards@honor.icsalabs.com](mailto:wizards@honor.icsalabs.com)

> Subject: RE: [fw-wiz] pixen abnormalities;

>

> That's a new one on me. You can use 'service resetoutside' and/or  
> 'service resetinbound' to cause the PIX to send an RST back to hosts  
> sending TCP packets that are denied by an access-list (or just denied  
in

> general). I don't know if this would result in connections that  
exceed

> the idle time set with the 'timeout' command receiving an RST or not.

I'd

> be interested to know how it behaves if anyone has tried this.

>

> PaulM

>

>

>> -----Original Message-----

>> It's ben awhile since I played in a firewall admin role, and worked  
> mostly

>> with fw-1 ipchains/iptables kinda setups. But, in a new position as  
a

>> unix/web admin, I'm dealing with firewall admins that maintain that  
not

>> setting the pixies to send an rst upon idel timeout is a  
'protection' in

Firewall-Wizards: RE: [fw-wiz] pixen abnormalities;

> > *case the connection that went idle was hijacked. Course, this will  
hose*  
> > *up a console connetion for a good twenty minutes or more depending  
upon*  
> > *the configuration of the sytems I'm using a console on. But, is  
this*  
> > *really a concern and rationale for not sending an rst on idle  
timeout*  
> > *limits?*  
> \_\_\_\_\_  
> *firewall-wizards mailing list*  
> *firewall-wizards@honor.icsalabs.com*  
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

\_\_\_\_\_  
firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>