

# Re: Lots of incoming traffic on UDP 1026 and UDP 1027?

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-12/0417.html>

---

*JGrimshaw\_at\_ASAP.com*

*Date:* 12/28/04

To: webmaster@focushacks.com

Date: Tue, 28 Dec 2004 11:39:04 -0600

I believe it's windows messenger traffic, most likely spam.

Search google for udp port 1026 and you'll get a lot of links regarding it. Activity to the windows messenger port seems to have been on the upswing since early December.

I know that ICQ (a chat program) used udp port 1027. That could be spam coming in, too.

FocusHacks <focushacks@gmail.com>

12/27/2004 12:34 PM

Please respond to

webmaster@focushacks.com

To

security-basics@securityfocus.com

cc

Subject

Lots of incoming traffic on UDP 1026 and UDP 1027?

I searched the archives at SecurityFocus and couldn't come up with anything useful other than someone with Zone Alarm obviously saw the same activity and people were trying to tell him to look for listening ports on his machine, which is not the case.

I'm getting literally hammered by tons of various IP's on UDP 1026 and UDP 1027

I've attached a CSV log, modified a bit, from my NetScreen 5. I only showed the last 15 bytes of the Source IP:Port so the first octet, give or take a few bytes, is cut off. I left a few columns out as well.

SecurityFocus BASICS: Re: Lots of incoming traffic on UDP 1026 and UDP 1027?

Let me know, this has been going on for quite a while, and all my searches are ending in vain. Any ideas?

--

<http://www.FocusHacks.com> - The Ford Focus Modification Site!

---

- application/octet-stream attachment: 1026-1027.csv