

## Re: CAN-2004-1137

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2005-01/0009.html>

---

**From:** Foundation Linux ([webmaster\\_at\\_foundationlinux.com](mailto:webmaster_at_foundationlinux.com))

**Date:** 01/05/05

Date: Wed, 05 Jan 2005 14:04:56 -0800  
To: hilton de meillon <[hiltond@hotpop.com](mailto:hiltond@hotpop.com)>

hilton de meillon wrote:

>Thanks a lot Charles and to all who replied. I will try these solutions and  
>see how I fare.  
>  
>I really need to touch up my TCP/IP or IGMP/IP skills.  
>  
>One question –your iptables statement had two entries – one for inbound igmp  
>and  
>one for outbound igmp, the first rule makes sense but the second one throws  
>me a bit  
>as it is in the INPUT chain and not the OUTPUT chain – is this just a lack  
>in my understanding of iptables ?.  
>  
>Hilton.  
>  
>

Actually, my example was limited to the INPUT chain but there was one for a SOURCE IP (coming from) and a DESTINATION IP (going to) 224.0.0.0/4. This covers anything coming from a multicast group and anything going to your multicast ports, even if they are routed to/from non-multicast IP addresses.

Unless you are running an IGMP daemon or something else that explicitly does multicast (or are really paranoid), you shouldn't have to worry about the OUTPUT chain.

Actually, the 224.0.0.0/4 range is not designed to be routed beyond one hop. Also, the source and destination routers associate normal IP addresses with the packets when routing the packets.

If you really want to understand IGMP, I suggest getting a copy of TCP/IP Illustrated Vol. I (ISBN: 0-201-63346-9). Chapter 13 is IGMP and Chapter 12 covers Broadcast & Multicast.

Good luck.

Charles Hill