

## Re: FreeBSD 5 ip\_gre and netisr\_enable=1

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2005-08/0196.html>

---

**From:** Max Laier (*max\_at\_love2party.net*)

**Date:** 08/25/05

To: freebsd-net@freebsd.org

Date: Thu, 25 Aug 2005 23:00:58 +0200

On Thursday 25 August 2005 22:10, ming fu wrote:

- > *Hi,*
- >
- > *This problem exit in some old gre.c (not a part of official freebsd) to*
- > *handle wccp packets. A carefully crafted packet can cause it to deplete*
- > *kernel stack and casuing a panic. It can crash a 4.2 kernel with about*
- > *200-300 repeated ip+gre header.*
- >
- > *I believe the problem appears on FreeBSD 5 with ip\_gre() and*
- > *net.isr.enable = 1. It probably easier to crash a 5.x because more calls*
- > *are involved in FreeBSD 5 than 4.x, thus more stack can be consumed with*
- > *the same repetition of headers.*
- >
- > *when a GRE packet gets into the ip\_gre2(), its gre header is stripped*
- > *and sent to netisr\_dispatch() for ip\_input() processing again. In case,*
- > *the net.isr.enable is 1, the packet will be delivered to ip\_input*
- > *directly instead of put in the queue.*
- >
- > *If someone create a packet consists of repeated ip and gre header,*
- >
- > *ip hdr : gre hdr : ip hdr : gre hdr : ..... repeat a few*
- > *hundred times.*
- >
- > *it can cause a loop around*
- > *ip\_gre->ip\_gre2->netisr\_dispatch->ip\_input->ip\_gre ..., not too*
- > *difficult to deplete the kernel stack.*
- >
- > *It only takes 24 bytes to force the kernel to go one round through these*
- > *calls.*
- >
- > *Any suggestion of how to fix this?*
- >
- > *send the gre stripped packet to netisr\_queue() is an easy, albeit slow*
- > *solution.*
- >
- > *I fix the older gre.c file by making sure the inner packet is not a GRE*

freebsd-net: Re: FreeBSD 5 ip\_gre and netisr\_enable=1

> *before deliver to ip\_input. However, it was ugly to parse the inner*  
> *header of in ip\_gre2().*

You could use an mbuf\_tag to keep track of recursion in the same way it is done in gif. There is certainly some overhead involved as well, however.

```
--  
/"\ Best regards, | mlaier@freebsd.org  
\ / Max Laier | ICQ #67774661  
X http://pf4freebsd.love2party.net/ | mlaier@EFnet  
/ \ ASCII Ribbon Campaign | Against HTML Mail and News
```

---

- application/pgp-signature attachment: stored