drivers: hamradio: 6pack: fix UAF bug caused by mod_timer()

Browse files

```
When a 6pack device is detaching, the sixpack_close() will act to cleanup
necessary resources. Although del_timer_sync() in sixpack_close()
won't return if there is an active timer, one could use mod_timer() in
sp_xmit_on_air() to wake up timer again by calling userspace syscall such
as ax25_sendmsg(), ax25_connect() and ax25_ioctl().

This unexpected waked handler, sp_xmit_on_air(), realizes nothing about
the undergoing cleanup and may still call pty_write() to use driver layer
resources that have already been released.

One of the possible race conditions is shown below:

      (USE)                      |      (FREE)
ax25_sendmsg()                   |
 ax25_queue_xmit()               |
  ...                            |
  sp_xmit()                      |
   sp_encaps()                   | sixpack_close()
    sp_xmit_on_air()             |  del_timer_sync(&sp->tx_t)
     mod_timer(&sp->tx_t,...)    |  ...
                                 |  unregister_netdev()
                                 |  ...
     (wait a while)              | tty_release()
                                 |  tty_release_struct()
                                 |   release_tty()
    sp_xmit_on_air()             |    tty_kref_put(tty_struct) //FREE
     pty_write(tty_struct) //USE |    ...

The corresponding fail log is shown below:
===============================================================
BUG: KASAN: use-after-free in __run_timers.part.0+0x170/0x470
Write of size 8 at addr ffff88800a652ab8 by task swapper/2/0
...
Call Trace:
  ...
  queue_work_on+0x3f/0x50
  pty_write+0xcd/0xe0pty_write+0xcd/0xe0
  sp_xmit_on_air+0xb2/0x1f0
  call_timer_fn+0x28/0x150
  __run_timers.part.0+0x3c2/0x470
  run_timer_softirq+0x3b/0x80
  __do_softirq+0xf1/0x380
  ...
```

```
This patch reorders the del_timer_sync() after the unregister_netdev()
to avoid UAF bugs. Because the unregister_netdev() is well synchronized,
it flushs out any pending queues, waits the refcount of net_device
decreases to zero and removes net_device from kernel. There is not any
running routines after executing unregister_netdev(). Therefore, we could
not arouse timer from userspace again.

Signed-off-by: Duoming Zhou <duoming@zju.edu.cn>
Reviewed-by: Lin Ma <linma@zju.edu.cn>
Signed-off-by: David S. Miller <davem@davemloft.net>
```

master

v6.1-rc6 … v5.17-rc6

stonezdm authored and **davem330** committed on Feb 18

1 parent 7a2fb91   commit efe4186e6a1b54bf38b9e05450d43b0da1fd7739

Showing **1 changed file** with **2 additions** and **2 deletions**.

Split | Unified

4 🟩🟩🟥🟥⬜ drivers/net/hamradio/6pack.c

```diff
 	 */
 	netif_stop_queue(sp->dev);
 
+	unregister_netdev(sp->dev);
+
 	del_timer_sync(&sp->tx_t);
 	del_timer_sync(&sp->resync_t);
 
-	unregister_netdev(sp->dev);
-
 	/* Free all 6pack frame buffers after unreg. */
 	kfree(sp->rbuff);
 	kfree(sp->xbuff);
```

0 comments on commit efe4186

Please sign in to comment.