author Duoming Zhou <duoming@zju.edu.cn> 2022-08-05 15:00:08 +0800
committer Jakub Kicinski <kuba@kernel.org> 2022-08-08 20:51:59 -0700
commit 3f4093e2bf4673f218c0bf17d8362337c400e77b (patch)
tree b8401e7acce01f755568d76eb4242bb6c9fed524
parent 7e4babffa6f340a74c820d44d44d16511e666424 (diff)
download ipsec-next-3f4093e2bf4673f218c0bf17d8362337c400e77b.tar.gz

diff options

context: 3
space: include
mode: unified

atm: idt77252: fix use-after-free bugs caused by tst_timer

```
There are use-after-free bugs caused by tst_timer. The root cause
is that there are no functions to stop tst_timer in idt77252_exit().
One of the possible race conditions is shown below:

     (thread 1)           |        (thread 2)
                          |   idt77252_init_one
                          |     init_card
                          |       fill_tst
                          |         mod_timer(&card->tst_timer, ...)
idt77252_exit             |   (wait a time)
                          |   tst_timer
                          |
                          |     ...
  kfree(card) // FREE     |
                          |     card->soft_tst[e] // USE

The idt77252_dev is deallocated in idt77252_exit() and used in
timer handler.

This patch adds del_timer_sync() in idt77252_exit() in order that
the timer handler could be stopped before the idt77252_dev is
deallocated.

Fixes: 1da177e4c3f4 ("Linux-2.6.12-rc2")
Signed-off-by: Duoming Zhou <duoming@zju.edu.cn>
Link: https://lore.kernel.org/r/20220805070008.18007-1-duoming@zju.edu.cn
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
```

Diffstat

-rw-r--r-- drivers/atm/idt77252.c 1

1 files changed, 1 insertions, 0 deletions

```
diff --git a/drivers/atm/idt77252.c b/drivers/atm/idt77252.c
index 81ce81a75fc67..681cb3786794d 100644
--- a/drivers/atm/idt77252.c
+++ b/drivers/atm/idt77252.c
@@ -3752,6 +3752,7 @@ static void __exit idt77252_exit(void)
                card = idt77252_chain;
                dev = card->atmdev;
                idt77252_chain = card->next;
+               del_timer_sync(&card->tst_timer);

                if (dev->phy->stop)
                        dev->phy->stop(dev);
```