Date: Sat, 2 Apr 2022 16:14:37 +0800 (GMT+08:00)
From: 周多明 <duoming@....edu.cn>
To: oss-security@...ts.openwall.com
Subject: CVE-2022-1205 kernel: Null pointer dereference and use-after-free
 in net/ax25/ax25_timer.c

Hello there,

There are NPD and use-after-free vulnerabilities in net/ax25/ax25_timer.c
of linux that allow attacker to crash linux kernel by simulating ax25 device
from user space.

=*=*=*=*=*=*=*=*=  Bug Details  =*=*=*=*=*=*=*=*=

There are race conditions that may lead to null pointer dereferences in
ax25_heartbeat_expiry(), ax25_t1timer_expiry(), ax25_t2timer_expiry(),
ax25_t3timer_expiry() and ax25_idletimer_expiry(), when we use
ax25_kill_by_device() to detach the ax25 device.

One of the race conditions that cause null pointer dereferences can be
shown as below:

```
      (Thread 1)                    |      (Thread 2)
ax25_connect()                      |
 ax25_std_establish_data_link()     |
  ax25_start_t1timer()              |
   mod_timer(&ax25->t1timer,..)     |
                                    | ax25_kill_by_device()
   (wait a time)                    |  ...
                                    |  s->ax25_dev = NULL; //(1)
   ax25_t1timer_expiry()            |
    ax25->ax25_dev->values[..] //(2)|  ...
     ...                            |
```

We set null to ax25_cb->ax25_dev in position (1) and dereference
the null pointer in position (2).

There are also race conditions that may lead to UAF bugs in
ax25_heartbeat_expiry(), ax25_t1timer_expiry(), ax25_t2timer_expiry(),
ax25_t3timer_expiry() and ax25_idletimer_expiry(), when we call
ax25_release() to deallocate ax25_dev.

```
      (Thread 1)                    |      (Thread 2)
ax25_dev_device_up() //(1)          |
...                                 | ax25_kill_by_device()
ax25_bind()          //(2)          |
ax25_connect()                      | ...
 ax25_std_establish_data_link()     |
  ax25_start_t1timer()              | ax25_dev_device_down() //(3)
   mod_timer(&ax25->t1timer,..)     |
                                    | ax25_release()
   (wait a time)                    |  ...
                                    |  ax25_dev_put(ax25_dev) //(4)FREE
   ax25_t1timer_expiry()            |
    ax25->ax25_dev->values[..] //USE|  ...
     ...                            |
```

We increase the refcount of ax25_dev in position (1) and (2), and
decrease the refcount of ax25_dev in position (3) and (4).
The ax25_dev will be freed in position (4) and be used in
ax25_t1timer_expiry().

=*=*=*=*=*=*=*=*=  Bug Effects  =*=*=*=*=*=*=*=*=

We can successfully trigger the NPD and UAF vulnerabilities to crash the linux kernel.

```
BUG: kernel NULL pointer dereference, address: 0000000000000050
CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc6-00794-g45690b7d0
RIP: 0010:ax25_t1timer_expiry+0x12/0x40
...
Call Trace:
 call_timer_fn+0x21/0x120
 __run_timers.part.0+0x1ca/0x250
 run_timer_softirq+0x2c/0x60
 __do_softirq+0xef/0x2f3
 irq_exit_rcu+0xb6/0x100
 sysvec_apic_timer_interrupt+0xa2/0xd0
...

================================================================

[  106.116942] BUG: KASAN: use-after-free in ax25_t1timer_expiry+0x1c/0x60
[  106.116942] Read of size 8 at addr ffff88800bda9028 by task swapper/0/0
[  106.116942] CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.17.0-06123-g0905eec574
[  106.116942] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-14
[  106.116942] Call Trace:
...
[  106.116942]  ax25_t1timer_expiry+0x1c/0x60
[  106.116942]  call_timer_fn+0x122/0x3d0
[  106.116942]  __run_timers.part.0+0x3f6/0x520
[  106.116942]  run_timer_softirq+0x4f/0xb0
[  106.116942]  __do_softirq+0x1c2/0x651
...

=*=*=*=*=*=*=*=  Bug Fix  =*=*=*=*=*=*=*=

The patch that have been applied to mainline Linux kernel is shown below.
https://github.com/torvalds/linux/commit/fc6d01ff9ef03b66d4a3a23b46fc3c3d8cf92009
https://github.com/torvalds/linux/commit/82e31755e55fbcea6a9dfaae5fe4860ade17cbc0

=*=*=*=*=*=*=*=  Timeline  =*=*=*=*=*=*=*=

2022-03-21: commit fc6d01ff9ef0 accepted to mainline kernel
2022-03-29: commit 82e31755e55f accepted to mainline kernel
2022-04-01: CVE-2022-1205 is assigned

=*=*=*=*=*=*=*=  Credit  =*=*=*=*=*=*=*=

Duoming Zhou <duoming@....edu.cn>

Best Regards,
Duoming Zhou
```