

[New issue](#)[Jump to bottom](#)

[Bug] Reachable assertion in packet2tree() #715

✓ Closed

Marsman1996 opened this issue on Feb 15 · 2 comments

Assignees



Labels

Cannot reproduce

Projects

4.4.2

Marsman1996 commented on Feb 15 • edited ▾

Describe the bug

The assertion `assert(121en > 0);` in `packet2tree()` at `tree.c` is reachable when the user uses `tcpprep` to open a crafted pcap file.

The variable `121en` is assigned in `get_l2len_protocol()` at `get.c`.

[tcpreplay/src/tree.c](#)

Lines 733 to 746 in 09f0774

```
733     res = get_l2len_protocol(data,
734                               pkt_len,
735                               datalink,
736                               &ether_type,
737                               &l2len,
738                               &l2offset,
739                               &vlan_offset);
740
741     if (res == -1)
742         goto len_error;
743
744     node = new_tree();
```

However, when the `datalink` is `DLT_RAW` or `DLT_JUNIPER_ETHER`, `121en` is assigned with 0, and the assertion is triggered.

[tcpreplay/src/common/get.c](#)

Lines 268 to 282 in 09f0774

```

268     *l2len = 0;
269     *l2offset = 0;
270     *vlan_offset = 0;
271
272     switch (datalink) {
273     case DLT_RAW:
274         if (datalen == 0)
275             return -1;
276
277         if ((pktdata[0] >> 4) == 4)
278             *protocol = ETHERTYPE_IP;
279         if ((pktdata[0] >> 4) == 6)

```

To Reproduce

Steps to reproduce the behavior:

1. Get the Tcppreplay source code (master [09f0774](#)) and compile it.
2. Run command: `$ tcpprep --auto=bridge --pcap=$POC --cachefile=/dev/null`

The POC file could be downloaded here:

[POC_file](#)

Expected behavior

Program reports assertion failure and is terminated.

Screenshots

```

> ./bin_normal/bin/tcpprep --auto=bridge --pcap=/crash/poc-tcppreplay-09f0774-packet2tree-assertion --cachefile=/dev/null
tcpprep: ../../code/src/tree.c:746: tcpr_tree_t *packet2tree(const u_char *, const int, int): Assertion `l2len > 0' failed.
[1] 26432 abort ./bin_normal/bin/tcpprep --auto=bridge --cachefile=/dev/null

```

The GDB report:

```

Breakpoint 6, packet2tree (data=0x7ffff7ef8010 "@", len=33, datalink=12) at
../../code/src/tree.c:733
733         res = get_l2len_protocol(data,
(gdb) p datalink
$8 = 12
(gdb) n
741         if (res == -1)
(gdb)
744         node = new_tree();
(gdb)

Breakpoint 1, packet2tree (data=0x7ffff7ef8010 "@", len=33, datalink=<optimized out>) at
../../code/src/tree.c:746
746         assert(l2len > 0);
(gdb) p l2len
$9 = 0
(gdb) c
Continuing.
tcpprep: ../../code/src/tree.c:746: tcpr_tree_t *packet2tree(const u_char *, const int, int):
Assertion `l2len > 0' failed.



```

Program received signal SIGABRT, Aborted.

```
0x00007ffff7194438 in __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:54
54      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
```

System (please complete the following information):

- OS: Ubuntu
- OS version: 16.04, 64 bit
- Tcpreplay Version: 4.4.1 (master [09f0774](#))

  **fklassen** added this to **To do** in **4.4.2** on Apr 22

  **fklassen** self-assigned this on Aug 1

  **fklassen** moved this from **To do** to **In progress** in **4.4.2** on Aug 1

fklassen commented on Aug 1



Member

Unable to recreate. What is your `./configure` command?

Here is my log:

```
$ ./configure --with-testnic=ens33
...
$ make
...
$ src/tcpprep --auto=bridge --pcap=$POC --cachefile=/dev/null


Fatal Error: Error opening file: invalid file capture length 264194, bigger than maximum of 262144
```

  **fklassen** added the **Cannot reproduce** label on Aug 1

fklassen commented on Aug 1

Member

Closing as "Cannot reproduce" however I believe that whatever you are seeing may be fixed with [#716](#).

 **fklassen** closed this as completed on Aug 1



4.4.2 automation moved this from In progress to Done on Aug 1



 5shadowblad3 mentioned this issue last month

[Bug] Reachable abort in tcpprep, packet2tree, src/tree.c:746 #756

 Open

Assignees



fklassen

Labels

Cannot reproduce

Projects



4.4.2

Done

Milestone

No milestone

Development

No branches or pull requests

2 participants

