[Bug] heap-overflow in get.c:344 #735

Closed **chluo911** opened this issue on Jul 24 · 1 comment

Assignees

Projects 4.4.2

chluo911 commented on Jul 24

You are opening a *bug report* against the Tcpreplay project: we use
GitHub Issues for tracking bug reports and feature requests.

If you have a question about how to use Tcpreplay, you are at the wrong
site. You can ask a question on the tcpreplay-users mailing list
or on Stack Overflow with [tcpreplay] tag.
General help is available here.

If you have a build issue, consider downloading the latest release

Otherwise, to report a bug, please fill out the reproduction steps
(below) and delete these introductory paragraphs. Thanks!

Describe the bug
A clear and concise description of what the bug is.
There is a heap-overflow bug in get_ipv6_next. Different from #716 (The crash point is in line 322, `ntohs(eth_hdr->ether_type);`), this bug is triggered in line 344 (`pktdata[12_net_off] >> 4`).

To Reproduce
Steps to reproduce the behavior:

1. export CC=clang && export CFLAGS="-fsanitize=address -g"
2. ./autogen.sh && ./configure --disable-shared --disable-local-libopts && make clean && make -j8
3. tcpprep --auto=bridge --pcap=POC --cachefile=/dev/null

Expected behavior
A clear and concise description of what you expected to happen.
The program does not crash.

Screenshots

If applicable, add screenshots to help explain your problem.

```
Warning: bug was captured using a snaplen of 18 bytes.  This may mean you have truncated packets.
=================================================================
==14130==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000022 at pc 0x0000004f
6832 bp 0x7ffe10b07c60 sp 0x7ffe10b07c58
READ of size 1 at 0x603000000022 thread T0
    #0 0x4f6831 in get_l2len_protocol /home/users/chluo/tcpreplay/src/common/get.c:344:18
    #1 0x4f70d6 in get_ipv4 /home/users/chluo/tcpreplay/src/common/get.c:442:11
    #2 0x4cd3a0 in process_raw_packets /home/users/chluo/tcpreplay/src/tcpprep.c:368:41
    #3 0x4cd3a0 in main /home/users/chluo/tcpreplay/src/tcpprep.c:144:23
    #4 0x7fa2ca63a09a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2409a)
    #5 0x41f4f9 in _start (/home/users/chluo/tcpreplay/src/tcpprep+0x41f4f9)

0x603000000022 is located 0 bytes to the right of 18-byte region [0x603000000010,0x603000000022)
allocated by thread T0 here:
    #0 0x4991cd in malloc (/home/users/chluo/tcpreplay/src/tcpprep+0x4991cd)
    #1 0x7fa2cae74ee6  (/usr/lib/x86_64-linux-gnu/libpcap.so.0.8+0x20ee6)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/users/chluo/tcpreplay/src/common/get.c:344:
18 in get_l2len_protocol
Shadow bytes around the buggy address:
  0x0c067fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c067fff8000: fa fa 00 00[02]fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
```

System (please complete the following information):

- OS: Debian
- OS version: buster
- Tcpreplay Version: `09f0774`

Additional context

Add any other context about the problem here.

POC

poc.zip

 **chluo911** changed the title ~~heap-overflow in get_l2len_protocol:344~~ [Bug] heap-overflow in get.c:344 on Jul 24

 **fklassen** self-assigned this on Aug 6

fklassen added this to **To do** in **4.4.2** via automation on Aug 6

fklassen commented on Aug 6 — Member

Fixed overflow in PR #744

👍 1

fklassen closed this as completed on Aug 6

4.4.2 automation moved this from **To do** to **Done** on Aug 6

fklassen added a commit that referenced this issue on Aug 26

`Bug #735 heap-overflow in get_l2len_protocol` `6a84081`

fklassen added a commit that referenced this issue on Aug 26

`Merge pull request #744 from appneta/Bug_#735_heap-overflow_get_c ...` `34a5fc1`

Assignees

fklassen

Labels

None yet

Projects

4.4.2
Done

Milestone

No milestone

Development

No branches or pull requests

2 participants