New issue

Jump to bottom

[Bug] heap-overflow in get.c:713 #734

Closed chluo911 opened this issue on Jul 23 · 1 comment

Assignees

Projects 4.4.2

chluo911 commented on Jul 23 • edited

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!

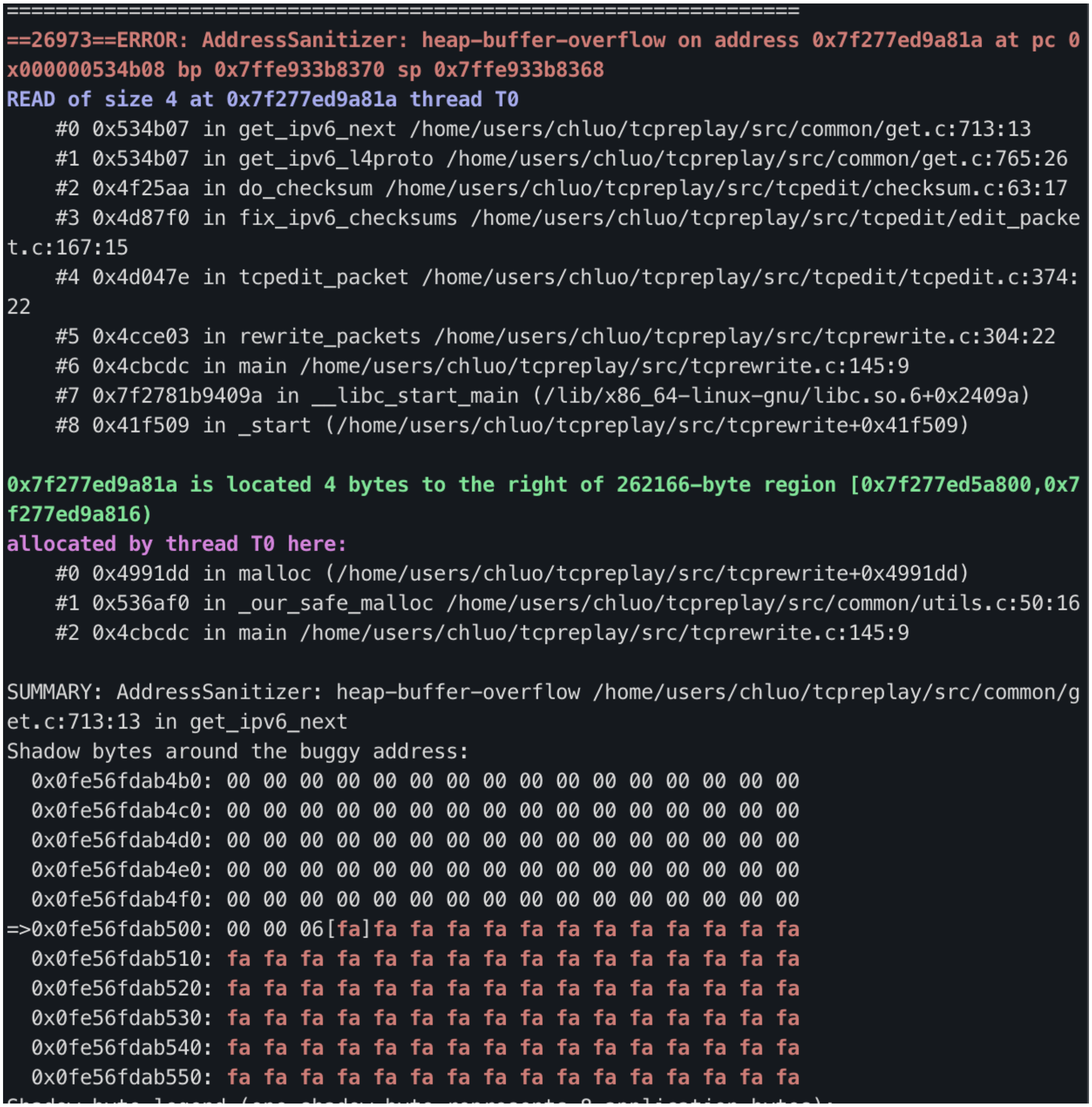
Describe the bug
There is a heap-overflow bug in get_ipv6_next. Different from #718 (The crash point is in line 679, `*((int*)((u_char *)exthdr + len))`), this bug is triggered in line 713 (`*((int*)((u_char *)exthdr + len)) > maxlen`).

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. ./src/tcprewrite -o /dev/null -i POC

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

Screenshots



```
=================================================================
==26973==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f277ed9a81a at pc 0
x000000534b08 bp 0x7ffe933b8370 sp 0x7ffe933b8368
READ of size 4 at 0x7f277ed9a81a thread T0
    #0 0x534b07 in get_ipv6_next /home/users/chluo/tcpreplay/src/common/get.c:713:13
    #1 0x534b07 in get_ipv6_l4proto /home/users/chluo/tcpreplay/src/common/get.c:765:26
    #2 0x4f25aa in do_checksum /home/users/chluo/tcpreplay/src/tcpedit/checksum.c:63:17
    #3 0x4d87f0 in fix_ipv6_checksums /home/users/chluo/tcpreplay/src/tcpedit/edit_packe
t.c:167:15
    #4 0x4d047e in tcpedit_packet /home/users/chluo/tcpreplay/src/tcpedit/tcpedit.c:374:
22
    #5 0x4cce03 in rewrite_packets /home/users/chluo/tcpreplay/src/tcprewrite.c:304:22
    #6 0x4cbcdc in main /home/users/chluo/tcpreplay/src/tcprewrite.c:145:9
    #7 0x7f2781b9409a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2409a)
    #8 0x41f509 in _start (/home/users/chluo/tcpreplay/src/tcprewrite+0x41f509)

0x7f277ed9a81a is located 4 bytes to the right of 262166-byte region [0x7f277ed5a800,0x7
f277ed9a816)
allocated by thread T0 here:
    #0 0x4991dd in malloc (/home/users/chluo/tcpreplay/src/tcprewrite+0x4991dd)
    #1 0x536af0 in _our_safe_malloc /home/users/chluo/tcpreplay/src/common/utils.c:50:16
    #2 0x4cbcdc in main /home/users/chluo/tcpreplay/src/tcprewrite.c:145:9

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/users/chluo/tcpreplay/src/common/g
et.c:713:13 in get_ipv6_next
Shadow bytes around the buggy address:
  0x0fe56fdab4b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe56fdab4c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe56fdab4d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe56fdab4e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe56fdab4f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe56fdab500: 00 00 06[fa]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe56fdab510: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe56fdab520: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe56fdab530: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe56fdab540: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe56fdab550: 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
POC
poc.zip

chluo911 changed the title ~~heap-overflow in get_ipv6_next:713~~ [BUG] heap-overflow in get_ipv6_next:713 on Jul 23

chluo911 changed the title ~~[BUG] heap-overflow in get_ipv6_next:713~~ [Bug] heap-overflow in get.c:713 on Jul 24

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

fklassen self-assigned this on Aug 6

fklassen moved this from **To do** to **In progress** in **4.4.2** on Aug 6

fklassen commented on Aug 6 Member

Tested with #718 fix. It appears that it is fixed.

fklassen closed this as completed on Aug 6

4.4.2 automation moved this from **In progress** to **Done** on Aug 6

Assignees

fklassen

Labels

None yet

Projects

4.4.2
Done

Milestone

No milestone

Development

No branches or pull requests

2 participants

2 participants