New issue

Jump to bottom

[Bug] heap-overflow in get.c:150 #736

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

chluo911 commented on Jul 24 • 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
A clear and concise description of what the bug is.
There is a heap-overflow bug in get.c:150. This bug is different from #719 that crashes in get.c:118.

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/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.

```
==15331==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000032 at pc 0x0000004f
5e95 bp 0x7ffe43018140 sp 0x7ffe43018138
READ of size 2 at 0x603000000032 thread T0
    #0 0x4f5e94 in parse_mpls /home/users/chluo/tcpreplay/src/common/get.c:150:26
    #1 0x4f5e94 in parse_metadata /home/users/chluo/tcpreplay/src/common/get.c:221:19
    #2 0x4f5e94 in get_l2len_protocol /home/users/chluo/tcpreplay/src/common/get.c:327:13
    #3 0x4f70d6 in get_ipv4 /home/users/chluo/tcpreplay/src/common/get.c:442:11
    #4 0x4cd3a0 in process_raw_packets /home/users/chluo/tcpreplay/src/tcpprep.c:368:41
    #5 0x4cd3a0 in main /home/users/chluo/tcpreplay/src/tcpprep.c:144:23
    #6 0x7f975092109a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2409a)
    #7 0x41f4f9 in _start (/home/users/chluo/tcpreplay/src/tcpprep+0x41f4f9)

0x603000000032 is located 11 bytes to the right of 23-byte region [0x603000000010,0x603000000027)
allocated by thread T0 here:
    #0 0x4991cd in malloc (/home/users/chluo/tcpreplay/src/tcpprep+0x4991cd)
    #1 0x7f975115bee6  (/usr/lib/x86_64-linux-gnu/libpcap.so.0.8+0x20ee6)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/users/chluo/tcpreplay/src/common/get.c:150:
26 in parse_mpls
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 07 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
```

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

fklassen commented on Aug 6 — Member

Fixed in #718

 **fklassen** closed this as completed on Aug 6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants