appneta / tcpreplay Public

Code | Issues 29 | Pull requests 5 | Actions | Projects 6 | Wiki | ...

New issue

Jump to bottom

Heap-buffer-overflow in tcpreplay #703

Closed ZFeiXQ opened this issue on Feb 5 · 1 comment · Fixed by #712

Assignees

Labels bug

Projects 4.4.1

ZFeiXQ commented on Feb 5

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
heap-buffer-overflow in tcpreplay

To Reproduce
Steps to reproduce the behavior:

1. export CFLAGS="-g -fsanitize=address" export CXXFLAGS="-g -fsanitize=address"
2. ./configure --disable-local-libopts
3. make
4. ./tcpreplay-edit -r 80:84 -s 20 -b -C -m 1500 -P --oneatatime -i lo POC2
5. POC2.zip

ASAN

```
=================================================================
==2505330==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000002a0 at pc 0x555db3af22a5 bp 0x7ffe70553580 sp 0x7ffe70553570
READ of size 2 at 0x6060000002a0 thread T0
    #0 0x555db3af22a4 in do_checksum_math /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/checksum.c:193
    #1 0x555db3af1be8 in do_checksum /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/checksum.c:103
    #2 0x555db3ae925c in fix_ipv4_checksums /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/edit_packet.c:81
    #3 0x555db3ae49b4 in tcpedit_packet /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/tcpedit.c:351
    #4 0x555db3acf3b9 in send_packets /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/send_packets.c:397
    #5 0x555db3ae0997 in replay_file /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/replay.c:182
    #6 0x555db3adf92b in tcpr_replay_index /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/replay.c:59
    #7 0x555db3ade6b8 in tcpreplay_replay /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpreplay_api.c:1139
    #8 0x555db3ad6f2a in main /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpreplay.c:178
    #9 0x7f5ea6e440b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x555db3ac916d in _start (/home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpreplay-edit+0x2016d)

0x6060000002a0 is located 0 bytes to the right of 64-byte region [0x606000000260,0x6060000002a0)
allocated by thread T0 here:
    #0 0x7f5ea718bbc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f5ea705720e  (/lib/x86_64-linux-gnu/libpcap.so.0.8+0x2420e)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/checksum.c:193 in do_checksum_math
Shadow bytes around the buggy address:
  0x0c0c7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c0c7fff8010: fd fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd
  0x0c0c7fff8020: fd fd fd fa fa fa fa fa 00 00 00 00 00 00 00 fa
  0x0c0c7fff8030: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c7fff8040: fd fd fd fd fd fd fd fd fa fa fa fa 00 00 00 00
=>0x0c0c7fff8050: 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff80a0: 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):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
```

```
    Poisoned by user:        f7
    Container overflow:      fc
    Array cookie:            ac
    Intra object redzone:    bb
    ASan internal:           fe
    Left alloca redzone:     ca
    Right alloca redzone:    cb
    Shadow gap:              cc
  ==2505330==ABORTING
```

System (please complete the following information):

- Ubuntu 20.04.1 LTS, gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)
- Tcpreplay Version [e.g. 4.3.2]

```
tcpreplay version: 4.4.0 (build git:v4.3.4-4-g0ca82e31)
Copyright 2013-2022 by Fred Klassen <tcpreplay at appneta dot com> - AppNeta
Copyright 2000-2012 by Aaron Turner <aturner at synfin dot net>
The entire Tcpreplay Suite is licensed under the GPLv3
Cache file supported: 04
Not compiled with libdnet.
Compiled against libpcap: 1.9.1
64 bit packet counters: enabled
Verbose printing via tcpdump: enabled
Packet editing: enabled
Fragroute engine: disabled
Injection method: PF_PACKET send()
Not compiled with netmap
```

fklassen self-assigned this on Feb 5

fklassen added the bug label on Feb 5

fklassen added this to **To do** in **4.4.1** on Feb 9

fklassen moved this from **To do** to **In progress** in **4.4.1** on Feb 11

fklassen added a commit that referenced this issue on Feb 11

`Bug #703 safeguard against corrupt packet lengths in checksum functions` e2ac765

✕

fklassen linked a pull request on Feb 11 that will close this issue

Bug #703 safeguard against corrupt packet lengths in checksum functions #712 Merged

fklassen added a commit that referenced this issue on Feb 12

`Bug #703 fix use-after-free on error messages` 7248ddb

fklassen added a commit that referenced this issue on Feb 12

`Bug #703 fix IP header lengths before checksum` ✓ b63f169

fklassen added a commit that referenced this issue on Feb 12

`Merge pull request #712 from appneta/Bug_#703_tcpreplay_heap-buffer-o…` … ✓ b388cbc

fklassen commented on Feb 12 Member

fixed in PR #712

fklassen closed this as completed on Feb 12

4.4.1 automation moved this from **In progress** to **Done** on Feb 12

Assignees

fklassen

Labels

bug

Projects

4.4.1
Done

Milestone

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Bug #703 safeguard against corrupt packet lengths in checksum functions
appneta/tcpreplay

2 participants