

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

[Bug] heap-overflow in get_ipv6_next #718

✓ Closed kdsjZh opened this issue on Mar 4 · 1 comment

Assignees



Projects

4.4.2

kdsjZh commented on Mar 4 • 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 found in get_ipv6_next, can be triggered via tcprewrite + ASan

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
- output:

Warning: tcprewrite/crash.1 was captured using a snaplen of 64 bytes. This may mean you have truncated packets.

=====

```
==7944==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fc3f2e48820 at pc
0x000000535bca bp 0x7ffe1d7fcb70 sp 0x7ffe1d7fcb68
READ of size 4 at 0x7fc3f2e48820 thread T0
#0 0x535bc9 in get_ipv6_next /benchmark/vulnerable/tcpreplay/src/common/get.c:679:14
#1 0x53598e in get_layer4_v6 /benchmark/vulnerable/tcpreplay/src/common/get.c:626:22
#2 0x4f9bc4 in tcpedit_packet /benchmark/vulnerable/tcpreplay/src/tcpedit/tcpedit.c:198:13
#3 0x4f80fc in rewrite_packets /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:304:22
#4 0x4f7418 in main /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:145:9

#5 0x7fc3f175dbf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-
start.c:310
#6 0x41c2c9 in _start (/benchmark/vulnerable/tcpreplay/src/tcprewrite+0x41c2c9)
```

0x7fc3f2e48820 is located 10 bytes to the right of 262166-byte region
[0x7fc3f2e08800,0x7fc3f2e48816)

allocated by thread T0 here:

```
#0 0x4aec90 in malloc /home/nipc/workspace/install/llvm-project/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x536c1f in _our_safe_malloc /benchmark/vulnerable/tcpreplay/src/common/utils.c:50:16
#2 0x4f7e02 in rewrite_packets /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:267:34
#3 0x4f7418 in main /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:145:9
#4 0x7fc3f175dbf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-
start.c:310
```

SUMMARY: AddressSanitizer: heap-buffer-overflow
/benchmark/vulnerable/tcpreplay/src/common/get.c:679:14 in get_ipv6_next

Shadow bytes around the buggy address:

```
0x0ff8fe5c10b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff8fe5c10c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff8fe5c10d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff8fe5c10e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff8fe5c10f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff8fe5c1100: 00 00 06 fa[fa]fa fa fa fa fa fa fa fa fa fa fa
0x0ff8fe5c1110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff8fe5c1120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff8fe5c1130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff8fe5c1140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff8fe5c1150: 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
==7944==ABORTING
```

Screenshots

```
nipc@root-pc:/benchmark/vulnerable/tcpreplay$ ./src/tcprewrite -o /dev/null -i tcprewrite/crash.1
Warning: tcprewrite/crash.1 was captured using a snaplen of 64 bytes. This may mean you have truncated packets.
=====
==7944==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fc3f2e48820 at pc 0x000000535bca bp 0x7ffe1d7fcb70 sp 0x7ffe1d7fcb68
READ of size 4 at 0x7fc3f2e48820 thread T0
#0 0x535bc9 in get_ipv6_next /benchmark/vulnerable/tcpreplay/src/common/get.c:679:14
#1 0x53598e in get_layer4_v6 /benchmark/vulnerable/tcpreplay/src/common/get.c:626:22
#2 0x4f9bc4 in tcpedit_packet /benchmark/vulnerable/tcpreplay/src/tcpedit/tcpedit.c:198:13
#3 0x4f80fc in rewrite_packets /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:304:22
#4 0x4f7418 in main /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:145:9

#5 0x7fc3f175dbf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-start.c:310
#6 0x41c2c9 in _start (/benchmark/vulnerable/tcpreplay/src/tcprewrite+0x41c2c9)

0x7fc3f2e48820 is located 10 bytes to the right of 262166-byte region [0x7fc3f2e08800,0x7fc3f2e48816)
allocated by thread T0 here:
#0 0x4aec90 in malloc /home/nipc/workspace/install/llvm-project/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x536c1f in _our_safe_malloc /benchmark/vulnerable/tcpreplay/src/common/utlis.c:50:16
#2 0x4f7e02 in rewrite_packets /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:267:34
#3 0x4f7418 in main /benchmark/vulnerable/tcpreplay/src/tcprewrite.c:145:9
#4 0x7fc3f175dbf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /benchmark/vulnerable/tcpreplay/src/common/get.c:679:14 in get_ipv6_next
Shadow bytes around the buggy address:
 0x0ff8fe5c10b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0ff8fe5c10c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0ff8fe5c10d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0ff8fe5c10e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0ff8fe5c10f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff8fe5c1100: 00 00 06 fa[fa]fa fa fa fa fa fa fa fa fa fa fa
 0x0ff8fe5c1110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0ff8fe5c1120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0ff8fe5c1130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0ff8fe5c1140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0ff8fe5c1150: 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
```

System (please complete the following information):

- OS: Ubuntu
- OS version : can be reproduced in 18.04/20.04
- clang version: 12.0.1 (release/12.x)
- Tcpreplay Version : latest commit [09f0774](#)

Credit

Han Zheng

[NCNIPC of China](#)

[Hexhive](#)

POC

[POC2.zip](#)

 fklassen added this to To do in 4.4.2 on Apr 22

 chluo911 mentioned this issue on Jul 23

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


✓ Closed

👤  fklassen self-assigned this on Aug 4

fklassen commented on Aug 4

Member

Improved overflow protection added in PR [#740](#)

 fklassen closed this as completed on Aug 4


📋 4.4.2 automation moved this from **To do** to **Done** on Aug 4

🔗  fklassen mentioned this issue on Aug 6

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

✓ Closed


🔗 fklassen added a commit that referenced this issue on Aug 26

 Bug [#718](#) improved heap-overflow protection ... 49420cb

🔗 fklassen added a commit that referenced this issue on Aug 26

 Merge pull request [#740](#) from appneta/Bug_#718_heap-overflow_in_get_ip... ... ad346b7

Assignees

 fklassen

Labels

None yet

Projects

📋 4.4.2
Done

Milestone

No milestone

Development

No branches or pull requests

2 participants

