[Bug] Double-free #702

Closed · **ZFeiXQ** opened this issue on Feb 5 · 2 comments · Fixed by #711

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
Double free 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. tcprewrite -i POC1 -o /dev/null

ASAN

```
Warning: ../../../POC1 was captured using a snaplen of 2 bytes.  This may mean you have truncated packets.
=================================================================
==1805053==ERROR: AddressSanitizer: attempting double-free on 0x60c0000001c0 in thread T0:
    #0 0x7ff303d557cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
    #1 0x56235e5df26c in _our_safe_free /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/common/utils.c:119
    #2 0x56235e5d5642 in dlt_jnpr_ether_cleanup plugins/dlt_jnpr_ether/jnpr_ether.c:171
    #3 0x56235e5c43f3 in tcpedit_dlt_cleanup plugins/dlt_plugins.c:463
    #4 0x56235e5b4968 in tcpedit_close /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/tcpedit.c:575
    #5 0x56235e5b08c1 in main /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcprewrite.c:147
    #6 0x7ff303a0e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #7 0x56235e5add2d in _start (/home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcprewrite+0x17d2d)

0x60c0000001c0 is located 0 bytes inside of 120-byte region [0x60c0000001c0,0x60c000000238)
freed by thread T0 here:
    #0 0x7ff303d557cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
    #1 0x56235e5df26c in _our_safe_free /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/common/utils.c:119
    #2 0x56235e5c4597 in tcpedit_dlt_cleanup plugins/dlt_plugins.c:480
    #3 0x56235e5d55ff in dlt_jnpr_ether_cleanup plugins/dlt_jnpr_ether/jnpr_ether.c:170
    #4 0x56235e5c43f3 in tcpedit_dlt_cleanup plugins/dlt_plugins.c:463
    #5 0x56235e5b4968 in tcpedit_close /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/tcpedit.c:575
    #6 0x56235e5b08c1 in main /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcprewrite.c:147
    #7 0x7ff303a0e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

previously allocated by thread T0 here:
    #0 0x7ff303d55bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x56235e5defba in _our_safe_malloc /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/common/utils.c:50
    #2 0x56235e5c2f16 in tcpedit_dlt_init plugins/dlt_plugins.c:130
    #3 0x56235e5d53d4 in dlt_jnpr_ether_post_init plugins/dlt_jnpr_ether/jnpr_ether.c:141
    #4 0x56235e5c3902 in tcpedit_dlt_post_init plugins/dlt_plugins.c:268
    #5 0x56235e5c3571 in tcpedit_dlt_post_args plugins/dlt_plugins.c:213
    #6 0x56235e5b7586 in tcpedit_post_args /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcpedit/parse_args.c:252
    #7 0x56235e5b042e in main /home/zxq/CVE_testing/ASAN-install/tcpreplay/src/tcprewrite.c:87
    #8 0x7ff303a0e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: double-free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf) in __interceptor_free
==1805053==ABORTING
```

System (please complete the following information):

- Ubuntu 20.04.1 LTS, gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)
- ./tcprewrite -V

```
tcprewrite 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
Fragroute engine: disabled
```

Additional context

Add any other context about the problem here.

ZFeiXQ commented on Feb 5 Author

POC1.zip

ZFeiXQ closed this as completed on Feb 5

ZFeiXQ reopened this on Feb 5

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 added a commit that referenced this issue on Feb 11

`Bug #702 fix double free in Juniper DLT` ✓ 9297ac2

fklassen added a commit that referenced this issue on Feb 11

`Bug #702 prevent double init in Juniper DLT` ✓ 45cb2ac

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

Bug #702 fix double free in Juniper DLT #711 Merged

fklassen added a commit that referenced this issue on Feb 11

`Merge pull request #711 from appneta/Bug_#702_double_free` … ✓ c23738f

fklassen commented on Feb 11 Member

Fixed in PR #711

fklassen closed this as completed on Feb 11

4.4.1 automation moved this from **To do** to **Done** on Feb 11

Assignees

fklassen

Labels

bug

Projects

4.4.1
Done

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Bug #702 fix double free in Juniper DLT
appneta/tcpreplay

2 participants