New issue

Jump to bottom

[Bug] Reachable assertion in get_layer4_v6 #717

Closed kdsjZh opened this issue on Mar 4 · 2 comments

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
The assertion `assert(ip6_hdr);` in `get_layer4_v6()` at `common/get.c` is reachable when the user uses tcprewrite to open a crafted pcap file.

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.0 was captured using a snaplen of 96 bytes.  This may mean you have
truncated packets.
```

```
tcprewrite: get.c:599: void *get_layer4_v6(const ipv6_hdr_t *, const int): Assertion `ip6_hdr'
failed.
Aborted
```

Expected behavior
Program reports assertion failure and is terminated.

Screenshots

```
nipc@root-pc:/benchmark/vulnerable/tcpreplay$ ./src/tcprewrite -o /dev/null -i tcprewrite/crash.0
Warning: tcprewrite/crash.0 was captured using a snaplen of 96 bytes.  This may mean you have truncated packets.
tcprewrite: get.c:599: void *get_layer4_v6(const ipv6_hdr_t *, const int): Assertion `ip6_hdr' failed.
Aborted
```

System (please complete the following information):

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

Credit
Han Zheng
NCNIPC of China
Hexhive

kdsjZh commented on Mar 4 — Author

POC1.zip

fklassen added this to **To do** in **4.4.2** on Apr 22

fklassen self-assigned this on Aug 1

fklassen moved this from **To do** to **In progress** in **4.4.2** on Aug 1

fklassen added a commit that referenced this issue on Aug 2

`Bug #717 avoid assertion in get_layer4_v6` `bac620d`

fklassen added a commit that referenced this issue on Aug 2

`Merge pull request #739 from appneta/Bug_#717_reachable_assertion_get…` ··· `ff643e9`

fklassen commented on Aug 2 Member

Fixed in PR #739. Added test for null pointer.

fklassen closed this as completed on Aug 2

4.4.2 automation moved this from **In progress** to **Done** on Aug 2

Assignees

fklassen

Labels

None yet

Projects

4.4.2
Done

Milestone

No milestone

Development

No branches or pull requests

2 participants