

## Fuzz job crash output: fuzz-2021-11-01-10735.pcap

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2021-11-01-10735.pcap>

stderr:

```
Input file: /var/managerie/managerie/Modbus_TCP_coll_d1_read.pcap

Build host information:
Linux runner-yq5rvme-project-7898047-concurrent-2 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64
Distributor ID: Ubuntu
Description: Ubuntu 20.04.3 LTS
Release: 20.04
Codename: focal

CI job ASan Managerie Fuzz, ID 1734535286:

Return value: 0

Dissector bug: 0

Valgrind error count: 0

Latest (but not necessarily the problem) commit:
55ba59cd Skinny: Resynced Skinny xml definition with code

Command and args: /builds/wireshark/wireshark/_install/bin/tshark -2 -nvxr
Running as user "root" and group "root". This could be dangerous.
AddressSanitizer:DEADLYSYNICAL
=====
==57617==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000a (pc 0x7fe075f4aef4 bp 0x7ff6462c25a0 sp 0x7ff6462c25a0)
==57617==The signal is caused by a READ memory access.
==57617==Hint: address points to the zero page.
#0 0x7fe075f4aef4 in dissect_modbus_response /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:1245:5
#1 0x7fe075f4995b in dissect_modbus /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:1691:13
#2 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#3 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#4 0x7fe077eb8360 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3268:8
#5 0x7fe077ead574 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3281:8
#6 0x7fe075f4e0d7 in dissect_mbtp_pdu_common /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:529:5
#7 0x7fe075f4e46a in dissect_mbtp_pdu /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:541:12
#8 0x7fe07691a228 in tcp_dissect_pdus /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:4134:13
#9 0x7fe075f4e3a1 in dissect_mbtp_common /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:802:5
#10 0x7fe075f499c3 in dissect_mbtp /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:811:12
#11 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#12 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#13 0x7fe077eb0ab3 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1448:8
#14 0x7fe07691b24b in decode_tcp_ports /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:6236:9
#15 0x7fe076919233 in process_tcp_payload /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:6320:13
#16 0x7fe07691f31c in desegment_tcp /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:3611:9
#17 0x7fe07691d121 in dissect_tcp_payload /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:6393:9
#18 0x7fe07692e522 in dissect_tcp /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:7366:17
#19 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#20 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#21 0x7fe077eb0ab3 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1448:8
#22 0x7fe075c2cb8e in ip_try_dissect /builds/wireshark/wireshark/build/./epan/dissectors/packet-ip.c:1817:7
#23 0x7fe075c310f7 in dissect_ip_v4 /builds/wireshark/wireshark/build/./epan/dissectors/packet-ip.c:2306:10
#24 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#25 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#26 0x7fe077eb0ab3 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1448:8
#27 0x7fe077eb1a2c in dissector_try_uint /builds/wireshark/wireshark/build/./epan/packet.c:1472:9
#28 0x7fe075811143 in dissect_ethertype /builds/wireshark/wireshark/build/./epan/dissectors/packet-ethertype.c:296:21
#29 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#30 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#31 0x7fe077eb8360 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3268:8
#32 0x7fe077ead574 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3281:8
#33 0x7fe07672668f in dissect_payload /builds/wireshark/wireshark/build/./epan/dissectors/packet-sll.c:414:4
#34 0x7fe07672ac0e in dissect_sll_common /builds/wireshark/wireshark/build/./epan/dissectors/packet-sll.c:518:3
#35 0x7fe07672a1fd in dissect_sll_v1 /builds/wireshark/wireshark/build/./epan/dissectors/packet-sll.c:547:9
#36 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#37 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#38 0x7fe077eb8360 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3268:8
#39 0x7fe075899c38 in dissect_frame /builds/wireshark/wireshark/build/./epan/dissectors/packet-frame.c:863:6
#40 0x7fe077eb77aa in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#41 0x7fe077eb1123 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#42 0x7fe077eb8360 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3268:8
#43 0x7fe077ead574 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3281:8
#44 0x7fe077eadc58 in dissect_record /builds/wireshark/wireshark/build/./epan/packet.c:622:3
#45 0x7fe077e80598 in epan_dissect_run_with_taps /builds/wireshark/wireshark/build/./epan/epan.c:629:2
#46 0x56029bd3fa25 in process_packet_second_pass /builds/wireshark/wireshark/build/./tshark.c:3246:5
#47 0x56029bd3de7d in process_cap_file_second_pass /builds/wireshark/wireshark/build/./tshark.c:3388:9
#48 0x56029bd3829c in process_cap_file /builds/wireshark/wireshark/build/./tshark.c:3658:28
#49 0x56029bd3d441 in main /builds/wireshark/wireshark/build/./tshark.c:2098:16
#50 0x7fe06a7850b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#51 0x56029bc3f4ad in _start (/builds/wireshark/wireshark/_install/bin/tshark+0x5f4ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /builds/wireshark/wireshark/build/./epan/dissectors/packet-mbtp.c:1245:56 in dissect_modbus_response
==57617==ABORTING

fuzz-test.sh stderr:
Running as user "root" and group "root". This could be dangerous.
```

no debug trace

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. [More information](#)

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. [Learn more](#)

Related merge requests 4

Modbus: Add null pointer checks

14932

Modbus: Add null pointer checks

14938

Modbus: Add null pointer checks













14939

Modbus: Add null pointer checks

14940

When these merge requests are accepted, this issue will be closed automatically.

Activity

-  [A Wireshark Gittab Utility](#) added [c31](#) [tshark](#) scoped label 1 year ago
-  [A Wireshark Gittab Utility](#) added [c31](#) label 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4932 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) made the issue visible to everyone 1 year ago
-  [Gerald Combs](#) closed via commit [b641b661](#) 1 year ago
-  [A Wireshark Gittab Utility](#) closed via merge request [4932 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4938 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4939 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4940 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in commit [e1efbe23](#) 1 year ago
-  [Gerald Combs](#) mentioned in commit [55c12cc7](#) 1 year ago
-  [Gerald Combs](#) mentioned in commit [9e453dd5](#) 1 year ago

Please [register](#) or [sign in](#) to reply