

Fuzz job crash output: fuzz-2021-10-31-6829.pcap

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2021-10-31-6829.pcap>

stderr:

```
Input file: /var/meragerie/meragerie/11137-kismet_drone_server.pcapng.gz

Build host information:
Linux runner-yq5rvme-project-7898047-concurrent-0 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:58:18 UTC 2021 x86_64 x86_64
Distributor ID: Ubuntu
Description: Ubuntu 20.04.3 LTS
Release: 20.04
Codename: focal

CI job ASan Meragerie Fuzz, ID 1733384355:

Return value: 0

Dissector bug: 0

Valgrind error count: 0

Latest (but not necessarily the problem) commit:
6a0e044e docs: Update documentation to use ',' as set separator


Command and args: /builds/wireshark/wireshark/_install/bin/tshark -2 -nVxr
Running as user "root" and group "root". This could be dangerous.
AddressSanitizer:DEADLYSYNOPSIS
=====
==43252==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fde84f77e6b bp 0x7ffff0878410 sp 0x7ffffd07f000)
==43252==The signal is caused by a READ memory access.
==43252==Hint: address points to the zero page.
#0 0x7fde84f77e6b in dissect_wlan_radio_phdr /builds/wireshark/wireshark/build/./epan/dissectors/packet-ieee80211-radio-phdr.c:11
#1 0x7fde84f77e64 in dissect_wlan_radio /builds/wireshark/wireshark/build/./epan/dissectors/packet-ieee80211-radio.c:11
#2 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#3 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#4 0x7fde872de4e0 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3300:8
#5 0x7fde872de454 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3313:8
#6 0x7fde84f88d5f in dissect_radiotap /builds/wireshark/wireshark/build/./epan/dissectors/packet-ieee80211-radiotap.c:11
#7 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#8 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#9 0x7fde872de4073 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1464:8
#10 0x7fde872de402 in dissector_try_uint /builds/wireshark/wireshark/build/./epan/packet.c:1488:9
#11 0x7fde85133a2 in dissect_kdsp_message /builds/wireshark/wireshark/build/./epan/dissectors/packet-kdsp.c:416:11
#12 0x7fde85d3ac24 in tcp_dissect_pdu /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:4167:13
#13 0x7fde8513d2ae in dissect_kdsp /builds/wireshark/wireshark/build/./epan/dissectors/packet-kdsp.c:533:3
#14 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#15 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#16 0x7fde872de4073 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1464:8
#17 0x7fde85d3c2a6 in decode_tcp_ports /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:6324:9
#18 0x7fde85d42923 in process_tcp_payload /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:6400:13
#19 0x7fde85d4031c in desegment_tcp /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:3635:9
#20 0x7fde85d3e121 in dissect_tcp_payload /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:6473:9
#21 0x7fde85d4f522 in dissect_tcp /builds/wireshark/wireshark/build/./epan/dissectors/packet-tcp.c:7446:17
#22 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#23 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#24 0x7fde872de4073 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1464:8
#25 0x7fde85d4d4ee in ip_try_dissect /builds/wireshark/wireshark/build/./epan/dissectors/packet-ip.c:1817:7
#26 0x7fde85952457 in dissect_ip_v4 /builds/wireshark/wireshark/build/./epan/dissectors/packet-ip.c:2386:10
#27 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#28 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#29 0x7fde872de4073 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1464:8
#30 0x7fde872de402 in dissector_try_uint /builds/wireshark/wireshark/build/./epan/packet.c:1488:9
#31 0x7fde84c30c73 in dissect_ethertype /builds/wireshark/wireshark/build/./epan/dissectors/packet-ethertype.c:296:21
#32 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#33 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#34 0x7fde872de4e0 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3300:8
#35 0x7fde872de454 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3313:8
#36 0x7fde84c2da70 in dissect_eth_common /builds/wireshark/wireshark/build/./epan/dissectors/packet-eth.c:576:5
#37 0x7fde84c2c5d7 in dissect_eth /builds/wireshark/wireshark/build/./epan/dissectors/packet-eth.c:882:5
#38 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#39 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#40 0x7fde872de400 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3300:8
#41 0x7fde84c09b08 in dissect_frame /builds/wireshark/wireshark/build/./epan/dissectors/packet-frame.c:863:6
#42 0x7fde872de4e4 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:755:9
#43 0x7fde872de4e3 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:848:9
#44 0x7fde872de400 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3300:8
#45 0x7fde872de454 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3313:8
#46 0x7fde872de0238 in dissect_record /builds/wireshark/wireshark/build/./epan/packet.c:622:3
#47 0x7fde872a3a78 in epan_dissect_run_with_taps /builds/wireshark/wireshark/build/./epan/epan.c:629:2
#48 0x55722b7c0a25 in process_packet_second_pass /builds/wireshark/wireshark/build/./tshark.c:3246:5
#49 0x55722b7bee7d in process_cap_file_second_pass /builds/wireshark/wireshark/build/./tshark.c:3388:9
#50 0x55722b7b929c in process_cap_file /builds/wireshark/wireshark/build/./tshark.c:3658:28
#51 0x55722b7b3441 in main /builds/wireshark/wireshark/build/./tshark.c:2098:16
#52 0x7fde799cf0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#53 0x55722b6e84ad 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-ieee80211-radio.c:841:9 in dissect_wlan_radio
==43252==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



 802.11 Radio: Add null pointer checks.


14931



 802.11 Radio: Add null pointer checks.


14933



 802.11 Radio: Add null pointer checks.

14934












 802.11 Radio: Add null pointer checks.

14935

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

Activity

-  [A Wireshark Gittab Utility](#) added [ci](#) [tshark](#) scoped label 1 year ago
-  [A Wireshark Gittab Utility](#) added [ci](#) [tshark](#) label 1 year ago
-  [Gerald Combs](#) made the issue visible to everyone 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4931 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) closed via commit [6b473c01](#) 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4933 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4934 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in merge request [4935 \(merged\)](#) 1 year ago
-  [Gerald Combs](#) mentioned in commit [ab3bb461](#) 1 year ago
-  [Gerald Combs](#) mentioned in commit [80281507](#) 1 year ago
-  [Gerald Combs](#) mentioned in commit [8f6d8c78](#) 1 year ago

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