

Fuzz job crash output: fuzz-2021-11-01-6716.pcap

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2021-11-01-6716.pcap>

stderr:

```
Input file: /var/managerie/managerie/attachment_ippush_print.pcapng

Build host information:
Linux runner-yq5rvme-project-7898047-concurrent-1 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 Managerie Fuzz, ID 1733660730:

Return value: 0

Dissector bug: 0

Valgrind error count: 0

Git commit
commit 9207c6f233c968030b058bf58aa97ee41a79f8ab
Author: Gerald Combs <gerald@wireshark.org>
Date: Sun Oct 31 16:35:20 2021 +0800

[Automatic update for 2021-10-31]

Update manuf, services enterprise numbers, translations, and other items.

Command and args: /builds/wireshark/wireshark/_install/bin/tshark -2 -nvx
Running as user "root" and group "root". This could be dangerous.
AddressSanitizer:DEADLYSIGNAL
=====
==64340==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x7f0a60f712fa bp 0x7ffcdeb329a0 sp 0x7ffcdeb329a0)
==64340==The signal is caused by a READ memory access.
==64340==Hint: address points to the zero page.
#0 0x7f0a60f712fa in dissect_ippush /builds/wireshark/wireshark/build/./epan/dissectors/packet-ippush.c:409:113
#1 0x7f0a63346831 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:720:9
#2 0x7f0a6333b660 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813:9
#3 0x7f0a6333af79 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:1413:8
#4 0x7f0a63eaeac28 in try_dissect_next_protocol /builds/wireshark/wireshark/build/./epan/dissectors/packet-usb.c:3670:1
#5 0x7f0a63eae510 in dissect_usb_payload /builds/wireshark/wireshark/build/./epan/dissectors/packet-usb.c:4621:19
#6 0x7f0a63e9de3b in dissect_usb_common /builds/wireshark/wireshark/build/./epan/dissectors/packet-usb.c:5309:5
#7 0x7f0a63eaeff2 in dissect_win32_usb /builds/wireshark/wireshark/build/./epan/dissectors/packet-usb.c:5311:5
#8 0x7f0a63346831 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:720:9
#9 0x7f0a6333b660 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813:9
#10 0x7f0a63343000 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3233:8
#11 0x7f0a60b070c26 in dissect_frame /builds/wireshark/wireshark/build/./epan/dissectors/packet-frame.c:783:6
#12 0x7f0a63346831 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/packet.c:720:9
#13 0x7f0a6333b660 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813:9
#14 0x7f0a63343000 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:3233:8
#15 0x7f0a63337684 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.c:3246:8
#16 0x7f0a63336e6f in dissect_record /builds/wireshark/wireshark/build/./epan/packet.c:594:3
#17 0x7f0a63305e88 in epan_dissect_run_with_taps /builds/wireshark/wireshark/build/./epan/epan.c:598:2
#18 0x55a3fa9b4157 in process_packet_second_pass /builds/wireshark/wireshark/build/./tshark.c:3250:5
#19 0x55a3fa92080e in process_cap_file_second_pass /builds/wireshark/wireshark/build/./tshark.c:3389:9
#20 0x55a3fa8c9b6e in process_cap_file /builds/wireshark/wireshark/build/./tshark.c:3650:28
#21 0x55a3fa864c8 in main /builds/wireshark/wireshark/build/./tshark.c:2102:16
#22 0x7f0a565540b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#23 0x55a3fa9b543d in _start /builds/wireshark/wireshark/_install/bin/tshark+0x5b43d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /builds/wireshark/wireshark/build/./epan/dissectors/packet-ippush.c:409:113 in dissect_ippush
==64340==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

3

IPPUSB: Add a pointer check

14936

IPPUSB: Add a pointer check.

14941

IPPUSB: Add a pointer check.

14942

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

Activity

- [A Wireshark Gitter Utility](#) added [cli tshark](#) scoped label 1 year ago
- [A Wireshark Gitter Utility](#) added [crash](#) label 1 year ago
- [Gerald Combs](#) made the issue visible to everyone 1 year ago

Gerald Combs

@geraldcombs

1 year ago

This was triggered on the 3.4 branch. I can duplicate this there, but not in master.

Owner

Gerald Combs

mentioned in merge request

14936 (merged)

1 year ago

Gerald Combs

closed via commit

72ad70c

1 year ago

Gerald Combs

mentioned in merge request

14941 (merged)

1 year ago

Gerald Combs

mentioned in merge request

14942 (merged)


1 year ago

Gerald Combs

mentioned in commit

8c0b20e0

1 year ago

 Gerald Combs mentioned in commit [a58cb43c](#) 1 year ago

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