Closed · Issue created 2 years ago by **A Wireshark GitLab Utility**

Buildbot crash output: fuzz-2020-10-27-8166.pcap

Problems have been found with the following capture file:

https://www.wireshark.org/download/automated/captures/fuzz-2020-10-27-8166.pcap

stderr:

```
Input file: /home/wireshark/menagerie/menagerie/xrite-i1displaypro-i1profiler.pcap.gz

Build host information:
Linux build6 4.15.0-122-generic #124-Ubuntu SMP Thu Oct 15 13:03:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic

Buildbot information:
BUILDBOT_WORKERNAME=fuzz-test
BUILDBOT_BUILDNUMBER=9
BUILDBOT_BUILDERNAME=Fuzz Test
BUILDBOT_URL=https://buildbot.wireshark.org/wireshark-3.4/
BUILDBOT_REPOSITORY=git@gitlab.com:wireshark/wireshark.git
BUILDBOT_GOT_REVISION=9837703a118dc45dbcb47485bf4d11556b3a8df4

Return value:  0

Dissector bug:  0

Valgrind error count:  0



Git commit
commit 9837703a118dc45dbcb47485bf4d11556b3a8df4
Author: Guy Harris <gharris@sonic.net>
Date:   Sat Oct 24 07:44:36 2020 +0000

    dumpcap: fix the macOS "no permission to capture" message.

    The macOS installer works differently from the way it did when that
    message was written (it's now a drag-install for Wireshark, with
    separate installers for ChmodBPF and for files to add the Wireshark
    binary directory to the default $PATH), and the macOS main screen now
    offers a "click this to install" link, running the ChmodBPF installer,
    if the user doesn't have permissions to capture.  Update the message
    to reflect that (although that's wrong if you directly run dumpcap or
    run it via TShark - this needs to be cleaned up in some fashion).

    Fix a capitalization error while we're at it.

    In the code that generates the main screen message to which the dumpcap
    message refers, add a comment saying that, if the main screen message
    changes, dumpcap's message should also be updated.


    (cherry picked from commit 4fd7983b04695bfc1ccf83b49559074bfd3a80d1)


Command and args: /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/install.asan/bin/tshark  -nVxr
================================================================
==14757==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x613000000a68 at pc 0x7f93cc418f3e bp 0x7fffe5b0dca0 sp
WRITE of size 1 at 0x613000000a68 thread T0
    #0 0x7f93cc418f3d in decode_bits_in_field /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/to
    #1 0x7f93cc3b8a95 in _proto_tree_add_bits_ret_val /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/..
    #2 0x7f93cc3b5749 in proto_tree_add_bits_ret_val /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../
    #3 0x7f93cc3b56db in proto_tree_add_bits_item /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epa
    #4 0x7f93cae414c6 in dissect_usb_hid_data /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/di
    #5 0x7f93cc30c3a4 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/..
    #6 0x7f93cc301279 in call_dissector_work /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pac
    #7 0x7f93cc300ba3 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/
    #8 0x7f93cae69596 in try_dissect_next_protocol /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../ep
    #9 0x7f93cae64f45 in dissect_usb_payload /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/dis
    #10 0x7f93cae5c99b in dissect_usb_common /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/dis
    #11 0x7f93cae65a22 in dissect_win32_usb /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/diss
    #12 0x7f93cc30c3a4 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/
    #13 0x7f93cc301279 in call_dissector_work /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #14 0x7f93cc308c50 in call_dissector_only /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #15 0x7f93c9b0ef16 in dissect_frame /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/dissecto
    #16 0x7f93cc30c3a4 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/
    #17 0x7f93cc301279 in call_dissector_work /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #18 0x7f93cc308c50 in call_dissector_only /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #19 0x7f93cc2fd374 in call_dissector_with_data /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../ep
    #20 0x7f93cc2fcb76 in dissect_record /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/packet.
    #21 0x7f93cc2cd198 in epan_dissect_run_with_taps /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../
    #22 0x55f785c45970 in process_packet_single_pass /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../
    #23 0x55f785c493fb in process_cap_file_single_pass /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/..
    #24 0x55f785c42c10 in process_cap_file /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../tshark.c:3
    #25 0x55f785c3c8dd in main /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../tshark.c:2056:16
    #26 0x7f93bdcfbb96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
    #27 0x55f785b38fa9 in _start (/home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/install.asan/bin/tshark+0x59fa9)

0x613000000a68 is located 0 bytes to the right of 360-byte region [0x613000000900,0x613000000a68)
allocated by thread T0 here:
    #0 0x55f785be4973 in __interceptor_malloc (/home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/install.asan/bin/tshark
    #1 0x7f93be75bab8 in g_malloc (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x51ab8)
    #2 0x7f93cc1e3c62 in wmem_strict_alloc /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/wmem/
    #3 0x7f93cc1da6d9 in wmem_alloc /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/wmem/wmem_cc
    #4 0x7f93cc1da70c in wmem_alloc0 /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/wmem/wmem_c
    #5 0x7f93cc418dd2 in decode_bits_in_field /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/to
    #6 0x7f93cc3b8a95 in _proto_tree_add_bits_ret_val /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/..
    #7 0x7f93cc3b5749 in proto_tree_add_bits_ret_val /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../
    #8 0x7f93cc3b56db in proto_tree_add_bits_item /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epa
    #9 0x7f93cae414c6 in dissect_usb_hid_data /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/di
    #10 0x7f93cc30c3a4 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/
    #11 0x7f93cc301279 in call_dissector_work /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #12 0x7f93cc300ba3 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/
    #13 0x7f93cae69596 in try_dissect_next_protocol /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../e
    #14 0x7f93cae64f45 in dissect_usb_payload /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/di
    #15 0x7f93cae5c99b in dissect_usb_common /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/dis
    #16 0x7f93cae65a22 in dissect_win32_usb /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/diss
    #17 0x7f93cc30c3a4 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/
    #18 0x7f93cc301279 in call_dissector_work /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #19 0x7f93cc308c50 in call_dissector_only /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #20 0x7f93c9b0ef16 in dissect_frame /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/dissecto
    #21 0x7f93cc30c3a4 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/
    #22 0x7f93cc301279 in call_dissector_work /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #23 0x7f93cc308c50 in call_dissector_only /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/pa
    #24 0x7f93cc2fd374 in call_dissector_with_data /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../ep
    #25 0x7f93cc2fcb76 in dissect_record /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/packet.
    #26 0x7f93cc2cd198 in epan_dissect_run_with_taps /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../
    #27 0x55f785c45970 in process_packet_single_pass /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../
    #28 0x55f785c493fb in process_cap_file_single_pass /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/..
    #29 0x55f785c42c10 in process_cap_file /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../tshark.c:3

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/build/cmbuild/../epan/
Shadow bytes around the buggy address:
  0x0c267fff80f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c267fff8100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c267fff8110: 00 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c267fff8130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c267fff8140: 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa
  0x0c267fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==14757==ABORTING
```

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 2

Relates to

- Buildbot crash output: fuzz-2020-10-28-9442.pcap
  #16967
- Buildbot crash output: fuzz-2020-10-31-4619.pcap
  #16975

Related merge requests 3

- epan: Limit our bits in decode_bits_in_field.
  !871
- epan: Limit our bits in decode_bits_in_field.
  !895
- epan: Limit our bits in decode_bits_in_field.
  !896

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

Activity

A Wireshark GitLab Utility added cli tshark scoped label 2 years ago

A Wireshark GitLab Utility added crash label 2 years ago

Jaap Keuter marked this issue as related to #16967 (closed) 2 years ago

Gerald Combs @geraldcombs · 2 years ago (Owner)

We're passing a large (512) data_size to proto_tree_add_bits_item.

Gerald Combs mentioned in merge request !871 (merged) 2 years ago

A Wireshark GitLab Utility closed via merge request !871 (merged) 2 years ago

Gerald Combs marked #16967 (closed) as a duplicate of this issue 2 years ago

Gerald Combs marked #16975 (closed) as a duplicate of this issue 2 years ago

Gerald Combs marked this issue as related to #16975 (closed) 2 years ago

Gerald Combs mentioned in commit c8fedf65 2 years ago

Gerald Combs mentioned in merge request !895 (merged) 2 years ago

Gerald Combs mentioned in merge request !896 (merged) 2 years ago

Gerald Combs mentioned in commit 61f17d3c 2 years ago