Bug 16368 - Buildbot crash output: randpkt-2020-02-05-7402.pcap

Status: RESOLVED FIXED
Alias: None
Product: Wireshark
Component: Dissection engine (libwireshark) (show other bugs)
Version: unspecified
Hardware: x86-64 Ubuntu
Importance: High Major (vote)
Target Milestone: ---
Assignee: Bugzilla Administrator
URL:
Depends on:
Blocks:

Reported: 2020-02-05 11:40 UTC by Buildbot Builder
Modified: 2020-02-27 22:17 UTC (History)
CC List: 0 users

See Also: ~~16383~~
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9430

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Buildbot Builder 2020-02-05 11:40:03 UTC **Description**

```
Problems have been found with the following capture file:

https://www.wireshark.org/download/automated/captures/randpkt-2020-02-05-7402.pcap

stderr:
Input file:

Build host information:
Linux build6 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64
x86_64 x86_64 GNU/Linux
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.3 LTS
Release:        18.04
Codename:       bionic

Buildbot information:
BUILDBOT_WORKERNAME=fuzz-test
BUILDBOT_BUILDNUMBER=28
BUILDBOT_BUILDERNAME=Fuzz Test
BUILDBOT_URL=http://buildbot.wireshark.org/wireshark-3.2/
BUILDBOT_REPOSITORY=ssh://wireshark-buildbot@code.wireshark.org:29418/wireshark
BUILDBOT_GOT_REVISION=33d0da9f6fa9225fbdb9c1c714d4af5056808f13

Return value:  1

Dissector bug:  0

Valgrind error count:  0



Git commit
commit 33d0da9f6fa9225fbdb9c1c714d4af5056808f13
Author: Guy Harris <guy@alum.mit.edu>
Date:   Fri Jan 31 16:39:37 2020 -0800

    Check for liblua-{version} as well as liblua{version}.

    FreeBSD packages install liblua-{version}.

    Change-Id: Ib28d2032a13baff9da42d61e3054a8b8e64b5cc9
    Reviewed-on: https://code.wireshark.org/review/35994
    Reviewed-by: Guy Harris <guy@alum.mit.edu>
    (cherry picked from commit 555279facbb2d154845a57069f56d1e9b0de44d6)
    Reviewed-on: https://code.wireshark.org/review/35995


Command and args: /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/install.asan/bin/tshark -nVxr

================================================================
==2623==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61d0001ac080 at
pc 0x7f977688f35e bp 0x7ffc61814440 sp 0x7ffc61814438
READ of size 1 at 0x61d0001ac080 thread T0
    #0 0x7f977688f35d in wimax_mac_calc_crc32 /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../plugins/epan/wimax/crc.c:122:31
    #1 0x7f9776856059 in wimax_decode_dlmapc /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../plugins/epan/wimax/msg_dlmap.c:2389:20
    #2 0x7f977684a558 in dissect_wimax_pdu_decoder
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../plugins/epan/wimax/wimax_pdu_decoder.c:119:15
    #3 0x7f97901cb6b4 in call_dissector_through_handle
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:706:9
    #4 0x7f97901c08f9 in call_dissector_work /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:799:9
    #5 0x7f97901c7f60 in call_dissector_only /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:3183:8
    #6 0x7f97901bc9f4 in call_dissector_with_data
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:3196:8
    #7 0x7f97901c7fa1 in call_dissector /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:3213:9
    #8 0x7f9776847fcf in pdu_burst_decoder /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../plugins/epan/wimax/packet-m2m.c:462:4
    #9 0x7f97768476e4 in dissect_m2m /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../plugins/epan/wimax/packet-m2m.c:263:6
    #10 0x7f97901cb6b4 in call_dissector_through_handle
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:706:9
    #11 0x7f97901c08f9 in call_dissector_work /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:799:9
    #12 0x7f97901c0223 in dissector_try_uint_new
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:1399:8
    #13 0x7f97901c0ccb in dissector_try_uint /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:1423:9
    #14 0x7f978db6c260 in dissect_ethertype /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/dissectors/packet-ethertype.c:264:21
    #15 0x7f97901cb6b4 in call_dissector_through_handle
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:706:9
    #16 0x7f97901c08f9 in call_dissector_work /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:799:9
    #17 0x7f97901c7f60 in call_dissector_only /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:3183:8
    #18 0x7f97901bc9f4 in call_dissector_with_data
```

```
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:3196:8
    #19 0x7f978db6904b in dissect_eth_common /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/dissectors/packet-eth.c:555:5
    #20 0x7f978db67b43 in dissect_eth /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/dissectors/packet-eth.c:831:5
    #21 0x7f97901cb6b4 in call_dissector_through_handle
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:706:9
    #22 0x7f97901c08f9 in call_dissector_work /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:799:9
    #23 0x7f97901c7f60 in call_dissector_only /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:3183:8
    #24 0x7f978dbf8cab in dissect_frame /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/dissectors/packet-frame.c:632:6
    #25 0x7f97901cb6b4 in call_dissector_through_handle
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:706:9
    #26 0x7f97901c08f9 in call_dissector_work /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:799:9
    #27 0x7f97901c7f60 in call_dissector_only /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../epan/packet.c:3183:8
    #28 0x7f97901bc9f4 in call_dissector_with_data
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:3196:8
    #29 0x7f97901bc1f6 in dissect_record /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/packet.c:580:3
    #30 0x7f9790l8c828 in epan_dissect_run_with_taps
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../epan/epan.c:599:2
    #31 0x55a14e4f7220 in process_packet_single_pass
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:3769:5
    #32 0x55a14e4f946e in process_cap_file_single_pass
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:3425:9
    #33 0x55a14e4f328c in process_cap_file /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:3580:26
    #34 0x55a14e4ee714 in main /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:2052:16
    #35 0x7f978260ab96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #36 0x55a14e3eb999 in _start (/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/install.asan/bin/tshark+0x5e999)

0x61d0001ac080 is located 0 bytes to the right of 2048-byte region
[0x61d0001ab880,0x61d0001ac080)
allocated by thread T0 here:
    #0 0x55a14e497363 in __interceptor_malloc (/home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/install.asan/bin/tshark+0x10a363)
    #1 0x7f978306aab8 in g_malloc (/usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0+0x51ab8)
    #2 0x55a14e4f90ab in process_cap_file_single_pass
/home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:3361:3
    #3 0x55a14e4f328c in process_cap_file /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:3580:26
    #4 0x55a14e4ee714 in main /home/wireshark/builders/wireshark-3.2-
fuzz/fuzztest/build/cmbuild/../tshark.c:2052:16
    #5 0x7f978260ab96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/wireshark/builders/wireshark-
3.2-fuzz/fuzztest/build/cmbuild/../plugins/epan/wimax/crc.c:122:31 in
wimax_mac_calc_crc32
Shadow bytes around the buggy address:
  0x0c3a8002d7c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a8002d7d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a8002d7e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a8002d7f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a8002d800: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c3a8002d810:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a8002d820: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a8002d830: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a8002d840: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a8002d850: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8002d860: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==2623==ABORTING

[ no debug trace ]
```

Gerrit Code Review 2020-02-07 19:19:40 UTC Comment 1

Change 36048 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36048

Gerrit Code Review 2020-02-07 19:58:19 UTC Comment 2

Change 36049 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36049

Gerrit Code Review 2020-02-07 19:58:32 UTC Comment 3

Change 36050 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36050

Gerrit Code Review 2020-02-07 19:58:52 UTC Comment 4

Change 36051 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36051

Gerrit Code Review 2020-02-07 19:59:07 UTC Comment 5

Change 36048 merged by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36048

Gerrit Code Review 2020-02-07 19:59:16 UTC **Comment 6**

Change 36049 merged by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36049

Gerrit Code Review 2020-02-07 19:59:26 UTC **Comment 7**

Change 36050 merged by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36050

Gerrit Code Review 2020-02-07 19:59:34 UTC **Comment 8**

Change 36051 merged by Gerald Combs:
WiMax DLMAP: Add a length check.

https://code.wireshark.org/review/36051

Gerrit Code Review 2020-02-13 17:16:02 UTC **Comment 9**

Change 36092 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

https://code.wireshark.org/review/36092

Gerrit Code Review 2020-02-13 17:16:18 UTC **Comment 10**

Change 36093 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

https://code.wireshark.org/review/36093

Gerrit Code Review 2020-02-13 17:19:01 UTC **Comment 11**

Change 36094 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

https://code.wireshark.org/review/36094