Bug 16672 - Buildbot crash output: fuzz-2020-07-01-11491.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: 2020-07-03 00:10 UTC by Buildbot Builder
Modified: 2020-08-12 17:17 UTC (History)
CC List: 0 users

See Also: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17498

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 2020-07-03 00:10:02 UTC **Description**

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

https://www.wireshark.org/download/automated/captures/fuzz-2020-07-01-11491.pcap

stderr:
Input file: /home/wireshark/menagerie/menagerie/produce.pcapng

Build host information:
Linux build6 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64
x86_64 x86_64 GNU/Linux
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:        18.04
Codename:       bionic

Buildbot information:
BUILDBOT_WORKERNAME=clang-code-analysis
BUILDBOT_BUILDNUMBER=5242
BUILDBOT_BUILDERNAME=Clang Code Analysis
BUILDBOT_URL=http://buildbot.wireshark.org/wireshark-master/
BUILDBOT_REPOSITORY=ssh://wireshark-buildbot@code.wireshark.org:29418/wireshark
BUILDBOT_GOT_REVISION=40f3c393c3e5bf257a40d6b217ea5999746ccf14

Return value:  0

Dissector bug:  0

Valgrind error count:  15



Git commit
commit 40f3c393c3e5bf257a40d6b217ea5999746ccf14
Author: Stig Bjørlykke <stig@bjorlykke.org>
Date:   Tue Jun 30 20:11:39 2020 +0200

    coap: Move dissection of payload before state tracking

    Change-Id: Icd8bce0a12167cc3edb3cb70fad5dd696af0b796
    Reviewed-on: https://code.wireshark.org/review/37623
    Petri-Dish: Stig Bjørlykke <stig@bjorlykke.org>
    Tested-by: Petri Dish Buildbot
    Reviewed-by: Stig Bjørlykke <stig@bjorlykke.org>


Command and args: ./tools/valgrind-wireshark.sh -b
/home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/install.plain/bin
==25862== Memcheck, a memory error detector
==25862== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==25862== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==25862== Command: /home/wireshark/builders/wireshark-master-
fuzz/clangcodeanalysis/install.plain/bin/tshark -nr
/fuzz/buildbot/clangcodeanalysis/valgrind-fuzz/fuzz-2020-07-01-11491.pcap
==25862==
==25862== Invalid read of size 8
==25862==    at 0x840ECD1: tvb_free_chain (tvbuff.c:123)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb60 is 0 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x840ED41: tvb_free_internal (tvbuff.c:98)
```

```
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb68 is 8 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x840ED54: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb68 is 8 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x8416B94: composite_free (tvbuff_composite.c:41)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb98 is 56 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0xD11C3F2: g_slice_free_chain_with_offset (in /usr/lib/x86_64-
linux-gnu/libglib-2.0.so.0.5600.4)
==25862==    by 0x8416B9B: composite_free (tvbuff_composite.c:41)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0efed8 is 8 bytes inside a block of size 16 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD11C431: g_slice_free_chain_with_offset (in /usr/lib/x86_64-
```

```
linux-gnu/libglib-2.0.so.0.5600.4)
==25862==    by 0x8416B9B: composite_free (tvbuff_composite.c:41)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11CEA3: g_slist_append (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x8416774: tvb_composite_append (tvbuff_composite.c:223)
==25862==    by 0x732E84A: decompress_lz4 (packet-kafka.c:1372)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid free() / delete / delete[] / realloc()
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD11C431: g_slice_free_chain_with_offset (in /usr/lib/x86_64-
linux-gnu/libglib-2.0.so.0.5600.4)
==25862==    by 0x8416B9B: composite_free (tvbuff_composite.c:41)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0efed0 is 0 bytes inside a block of size 16 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD11C431: g_slice_free_chain_with_offset (in /usr/lib/x86_64-
linux-gnu/libglib-2.0.so.0.5600.4)
==25862==    by 0x8416B9B: composite_free (tvbuff_composite.c:41)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11CEA3: g_slist_append (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x8416774: tvb_composite_append (tvbuff_composite.c:223)
==25862==    by 0x732E84A: decompress_lz4 (packet-kafka.c:1372)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x8416BA0: composite_free (tvbuff_composite.c:43)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfba0 is 64 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x8416BAD: composite_free (tvbuff_composite.c:44)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfba8 is 72 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
```

```
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x8416BBA: composite_free (tvbuff_composite.c:45)
==25862==    by 0x840ED61: tvb_free_internal (tvbuff.c:99)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb80 is 32 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid read of size 8
==25862==    at 0x840ED66: tvb_free_internal (tvbuff.c:101)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb68 is 8 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862== Invalid free() / delete / delete[] / realloc()
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x839D88F: epan_dissect_reset (epan.c:544)
==25862==    by 0x127973: process_packet_single_pass (tshark.c:3789)
==25862==    by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
==25862==    by 0x1267C4: process_cap_file (tshark.c:3560)
==25862==    by 0x123CCD: main (tshark.c:2044)
==25862==  Address 0x1b0bfb60 is 0 bytes inside a block of size 80 free'd
==25862==    at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862==    by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862==    by 0x732E8B5: decompress_lz4 (packet-kafka.c:1385)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==    by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
==25862==    by 0x732D28D: dissect_kafka_produce_request_topic (packet-
kafka.c:2994)
==25862==  Block was alloc'd at
==25862==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==25862==    by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
```

```
2.0.so.0.5600.4)
==25862==    by 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==25862==    by 0x840EBD7: tvb_new (tvbuff.c:75)
==25862==    by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
==25862==    by 0x732E5D5: decompress_lz4 (packet-kafka.c:1308)
==25862==    by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862==    by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
==25862==    by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862==    by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862==    by 0x732D48C: dissect_kafka_produce_request_partition (packet-
kafka.c:2973)
==25862==    by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862==
==25862==
==25862== HEAP SUMMARY:
==25862==     in use at exit: 43,319 bytes in 204 blocks
==25862==   total heap usage: 330,264 allocs, 330,063 frees, 40,608,136 bytes
allocated
==25862==
==25862== LEAK SUMMARY:
==25862==    definitely lost: 0 bytes in 0 blocks
==25862==    indirectly lost: 0 bytes in 0 blocks
==25862==      possibly lost: 304 bytes in 1 blocks
==25862==    still reachable: 42,212 bytes in 170 blocks
==25862==         suppressed: 803 bytes in 33 blocks
==25862== Rerun with --leak-check=full to see details of leaked memory
==25862==
==25862== For counts of detected and suppressed errors, rerun with: -v
==25862== ERROR SUMMARY: 15 errors from 11 contexts (suppressed: 0 from 0)

[ no debug trace ]
```

Gerrit Code Review 2020-07-04 15:24:34 UTC **Comment 1**

Change 37696 had a related patch set uploaded by Martin Kaiser:
kafka: lz4: free the composite tvb only once

https://code.wireshark.org/review/37696

Gerrit Code Review 2020-07-05 12:14:10 UTC **Comment 2**

Change 37696 merged by Anders Broman:
kafka: lz4: free the composite tvb only once

https://code.wireshark.org/review/37696

Gerrit Code Review 2020-07-05 21:04:26 UTC **Comment 3**

Change 37720 had a related patch set uploaded by Guy Harris:
kafka: lz4: free the composite tvb only once

https://code.wireshark.org/review/37720

Gerrit Code Review 2020-07-05 21:04:35 UTC **Comment 4**

Change 37720 merged by Guy Harris:
kafka: lz4: free the composite tvb only once

https://code.wireshark.org/review/37720