# 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 (<u>History</u>)

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  $\underline{\log\,\mathrm{in}}$  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: 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\_BUILDENNAME=Clang Code Analysis BUILDBOT\_BUILDENNAME=Clang Code Analysis BUILDBOT\_URL=http://buildbot.wireshark.org/wireshark-master/ BUILDBOT\_EPOSITORY=ssh://wireshark-buildbot@code.wireshark.org:29418/wireshark BUILDBOT\_GOT\_REVISION=40f3c393c3e5bf257a40d6b217ea5999746ccf14 Return value: 0 Dissector bug: 0 Valgrind error count: 15 Git commit Stig Bjørlykke <stig@bjorlykke. Tue Jun 30 20:11:39 2020 +0200 coap: Move dissection of payload before state tracking Reviewed-on: https://code.wireshark.org/review/3 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 GRL'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-masterfuzz/clangcodeanalysis/install.plain/bin/tshark -nr /fuzz/buildbot/clangcodeanalysis/valgrind-fuzz/fuzz-2020-07-01-11491.pcap =25862= =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 0x73ZEBB: decompress 124 (packet-kafka.c:1385) by 0x73ZEIC1: decompress (packet-kafka.c:1385) by 0x73ZEIC1: decompress (packet-kafka.c:1549) by 0x73ZEIC1: decompress (packet-kafka.c:1549) by 0x73ZEIC1: decompress (packet-kafka.c:1797) by 0x73ZD3D5E: dissect kafka message (packet-kafka.c:1777) by 0x73ZD5FB: dissect kafka message (packet-kafka.c:1797) by 0x73ZD5FB: dissect kafka produce request partition (packet-kafka.c:2737) =25862= by 0x73ZD3D35: dissect kafka array\_fe (packet-kafka.c:907) =25862= by 0x73ZD3D35: dissect kafka array\_fe (packet-kafka.c:923) by 0x73ZD2B1: dissect kafka\_raray\_fe (packet-kafka.c:923) =25862= by 0x73ZD2B1: dissect\_kafka\_raray\_fe (packet-kafka.c:923) =25862= by 0x73ZD2B1: dissect\_kafka\_produce\_request\_partition (packet-kafka.c:2994) =25862= Block was alloc'd at =25862= at 0x4C2FB0F: malloc (in /usr/lib/vaff.fb.lieuv.gm/(lib/dib. ==25862== block was alloc'd at ==25862== at 0x4C2PBOF: malloc (in /usr/lib/valgrind/vgpreload\_memcheck-amd64 linux.so) ==25862== by 0xD103AB8: g\_malloc (in /usr/lib/x86\_64-linux-gnu/libglib2.0.so.0.5600.4) ==25862== by 0xD11B955: g\_slice\_alloc (in /usr/lib/x86\_64-linux-gnu/libglib2.0.so.0.5600.4) ==25862== by 0xB40EBD7: tvb\_new (tvbuff.c:75) ==25862== by 0x840EBD7: tvb\_new (composite (tvbuff\_composite.c:197) ==25862== by 0x73ZE5D5: decompress [24 (packet-kafka.c:1308) ==25862== by 0x73ZE5D5: decompress [24 (packet-kafka.c:1308) ==25862== by 0x73ZE5D5: dissect kafka message old (packet-kafka.c:1776) ==25862== by 0x73ZD575: dissect kafka message set (packet-kafka.c:1776) ==25862== by 0x73ZD575: dissect kafka message set (packet-kafka.c:1797) ==25862== by 0x73ZD575: dissect kafka message set (packet-kafka.c:1797) ==25862== by 0x73ZD575: dissect kafka message set (packet-kafka.c:1797) ==25862== by 0x73ZD575: dissect kafka message set (packet-kafka.c:2797) ==25862== by 0x73ZD575: dissect kafka message set (packet-kafka.c:907) ==25862== livalid read of size 8 ==25862== livalid read of size 8 ==25862== livalid read of size 8

```
by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
by 0x839D88F: epan_dissect_reset (epan.c:544)
by 0x12973: process_packet_single_pass (tshark.c:3789)
by 0x1292ED: process_cap_file_single_pass (tshark.c:3405)
by 0x1267C4: process_cap_file_(tshark.c:3560)
by 0x123CCD: main (tshark.c:2044)
Address 0x1bobfb68 is 8 bytes inside a block of size 80 free'd
at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
    ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
                                                       by 0x840ED80: tvb_free_internal (tvbuff.c:103)
by 0x840ED80: tvb_free_chain (tvbuff.c:124)
by 0x73ZEB85: decompress 124 (packet-kafka.c:1385)
by 0x73ZEB1c1: decompress (packet-kafka.c:1549)
by 0x73ZD9E5: dissect kafka message old (packet-kafka.c:1633)
by 0x73ZD9T3c: dissect kafka message (packet-kafka.c:1776)
by 0x73ZD9T8: dissect_kafka message set (packet-kafka.c:1779)
by 0x73ZD48C: dissect_kafka produce_request_partition (packet-))
    linux.so)
     ==25862==
     ==25862==
    kafka.c:2973)
                                                        )
by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
by 0x732D28D: dissect_kafka_produce_request_topic (packet-
     ==25862==
==25862==
     ==25862==
    kafka.c:2994)
    ==25862== Block was alloc'd at
==25862== at 0x4C2FB0F: mail
                                                       at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload memcheck-amd64-
   ==25862== by 0xDl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
   ==25862== by OxDl1B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
 2.0.so.0.5600.4)

==25862== by 0x840EBD7: tvb_new (tvbuff.c:75)

==25862== by 0x8416643: tvb_new composite (tvbuff_composite.c:197)

by 0x732ED5: decompress 1z4 (packet-kafka.c:1308)

==25862== by 0x732E1C1: decompress [packet-kafka.c:1549]

==25862== by 0x732D95: dissect kafka message old (packet-kafka.c:1776)

==25862== by 0x732D73C: dissect kafka message (packet-kafka.c:1797)

==25862== by 0x732D48C: dissect kafka message (packet-kafka.c:1797)

==25862== by 0x732D48C: dissect kafka message set (packet-kafka.c:1797)

==25862== by 0x732D48C: dissect kafka message set (packet-kafka.c:1797)

==25862== by 0x732D48C: dissect kafka produce_request_partition (packet-kafka.c:2973)

by 0x732D395: dissect kafka produce_request_partition (packet-kafka.c:2973)
 =25862= by 0x732D395: dissect_karka_produce_lequest_partition (packet-karka.c:2973)
=25862= by 0x732D395: dissect_karka_array_ref (packet-karka.c:907)
=25862= lnvalid read of size 8
=25862= by 0x840DES91: tvb_free_internal (tvbuff.c:124)
=25862= by 0x840DEC80: tvb_free_chain (tvbuff.c:124)
=25862= by 0x840DEC80: tvb_free_chain (tvbuff.c:124)
=25862= by 0x127973: process_packet_single_pass (tshark.c:3789)
=25862= by 0x1229D: process_cap_file_single_pass (tshark.c:3405)
=25862= by 0x123CCD: main (tshark.c:2044)
=25862= by 0x123CCD: main (tshark.c:2044)
=25862= Address 0x1b0bfb68 is 8 bytes inside a block of size 80 free'd
=25862= by 0x300D38: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
=25862= by 0x732D855: dissect_karka_c:1249)
=25862= by 0x732D855: dissect_karka_message (packet-karka.c:1633)
=25862= by 0x732D955: dissect_karka_message (packet-karka.c:1797)
=25862= by 0x732D5781: dissect_karka_message (packet-karka.c:1797)
                                                      by 0x840ED80: tvb_free_internal (tvbuff.c:103)
by 0x840ECR0: tvb_free_chain (tvbuff.c:124)
by 0x73ZE885: decompress 124 (packet-kafka.c:1385)
by 0x73ZEB1c1: decompress (packet-kafka.c:1549)
by 0x73ZD9E5: dissect kafka_message_old (packet-kafka.c:1633)
by 0x73ZD57B: dissect_kafka_message (packet-kafka.c:1776)
by 0x73ZD57B: dissect_kafka_message set (packet-kafka.c:1797)
by 0x73ZD58C: dissect_kafka_produce_request_partition (packet-
3)
    ==29862== by UX/32D48C: dissect_kafka_produce_lequest_partition_(pac.

==25862== by UX/32D184: dissect_kafka_array_(packet-kafka_c:907)

==25862== by UX/32D184: dissect_kafka_array_(packet-kafka_c:923)

==25862== by UX/32D184: dissect_kafka_produce_request_topic_(packet-

before_array_0204)
   ==25862==
kafka.c:2994)
==25862==
B1
==25862==
                                              Block was alloc'd at
at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
        =25862== by 0xbl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-

-2.5862== by 0xbl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-

-2.5862== by 0xbl1bacc - . .
        DO.4)
by 0x840EBD7: tvb_new (tvbuff.c:75)
by 0x8416643: tvb_new composite (tvbuff_composite.c:197)
by 0x73ZE5D5: decompress 124 (packet-kafka.c:1308)
by 0x73ZEB1c1: decompress (packet-kafka.c:1549)
by 0x73ZD9E5: dissect kafka_message old (packet-kafka.c:1633)
by 0x73ZD57B: dissect kafka_message (packet-kafka.c:1776)
by 0x73ZD57B: dissect kafka_message set (packet-kafka.c:1797)
by 0x73ZD57B: dissect_kafka_produce_request_partition (packet-
3)
    kafka.c:2973)
==25862==
                                                         by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
  --23862= Invalid read of size 8
--25862= at 0x8416894: composite free (tvbuff_composite.c:41)
by 0x840ECB0: tvb free Internal (tvbuff.c:99)
--25862= by 0x840ECB0: tvb free chain (tvbuff.c:124)
by 0x839088F: epan dissect reset (epan.c:544)
--25862= by 0x127973: process_packet single_pass (tshark.c:3789)
--25862= by 0x12292ED: process_cap_file_single_pass (tshark.c:3405)
--25862= by 0x123CCD: main (tshark.c:3204)
--25862= at 0x4c30038: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
     ==25862== Invalid read of size 8
    linux.so)
==25862==
                                                      by 0x840ED80: tvb_free_internal (tvbuff.c:103)
by 0x840EC80: tvb_free_chain (tvbuff.c:124)
by 0x73ZEB85: decompress 124 (packet-kafka.c:1385)
by 0x73ZED85: dissect_kafka.message_old (packet-kafka.c:1633)
by 0x73ZD73C: dissect_kafka_message_ (packet-kafka.c:1776)
by 0x73ZD57B: dissect_kafka_message_set (packet-kafka.c:1777)
by 0x73ZD57B: dissect_kafka_produce_request_partition (packet-
3)
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
   ==25862== by 0x732D184: dissect_kafka_array_ref (packet-kafka.c:907)
==25862= by 0x732D184: dissect_kafka_array_ref (packet-kafka.c:907)
==25862= by 0x732D184: dissect_kafka_array_(packet-kafka.c:923)
==25862= by 0x732D184: dissect_kafka_produce_request_topic (packet-
   --25862== Block was alloc'd at
==25862= at 0x4C2FB0F: mall
                                                        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 0xD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)

2.0.so.0.5602= by 0x840EBD7: tvb_new (tvbuff.c:75)
=25862== by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
=25862== by 0x32ED51: decompress 124 (packet-kafka.c:1308)
=25862== by 0x732ED1: decompress (packet-kafka.c:1549)
=25862== by 0x732D95E: dissect_kafka_message (packet-kafka.c:176)
=25862== by 0x732D78C: dissect_kafka_message (packet-kafka.c:1776)
=25862== by 0x732D78C: dissect_kafka_message (packet-kafka.c:1777)
=25862== by 0x732D5FE: dissect_kafka_message set_(packet-kafka.c:1797)
=25862== by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:1973)
=25862== by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:1973)
=25862== by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:1973)
=25862== at 0xD103P2: g_slice_free_chain_with_offset (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
=25862== by 0x840EB61: tvb_free_internal (tvbuff.c:194)
=25862== by 0x840EB61: tvb_free_chain_(tvbuff.c:194)
=25862== by 0x840EB61: tvb_free_chain_(tvbuff.c:194)
=25862== by 0x840EB61: tvb_free_chain_(tvbuff.c:194)
=25862== by 0x127973: process_packet_single_pass_(tshark.c:3789)
=25862== by 0x127973: process_packet_single_pass_(tshark.c:3789)
=25862== by 0x1267C4: process_cap_file_single_pass_(tshark.c:3789)
=25862== by 0x1267C4: process_cap_file_tshark.c:360)
by 0x123CCb: main (tshark.c:2044)
=25862== by 0x123CCb: main (tshark.c:2044)
=25862== at 0x403D3B: free_cin/usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
=25862== by 0xD11C431: g_slice_free_chain_with_offset_(in /usr/lib/x86_64-linux.so)
   linux.so)
==25862==
                                                         by 0xD11C431: g_slice_free_chain_with_offset (in /usr/lib/x86_64-
```

```
linux-qnu/libqlib-2.0.so.0.5600.4)
                                               bglib-2.0.so.0.5600.4)
by 0x841689B: composite free (tvbuff_composite.c:41)
by 0x840ED61: tvb_free_internal (tvbuff.c:99)
by 0x840ECE0: tvb_free_internal (tvbuff.c:124)
by 0x732E085: decompress 124 (packet-kafka.c:1385)
by 0x732E1C1: decompress [packet-kafka.c:1549)
by 0x732D955: dissect_kafka_message_old (packet-kafka.c:1776)
by 0x732D75E: dissect_kafka_message [packet-kafka.c:17770]
by 0x732D75E: dissect_kafka_produce_request_partition (packet-)
    ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
    kafka.c:2973)
                                               n)
by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
llock was alloc'd at
at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
     ==25862== by (
==25862== Block
     ==25862==
   inux.so) ==25862= by 0xDl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4) ==25862= by 0xDl1B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
   ==25862== by OxDllCEA3: g_slist_append (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
 2.0.so.0.5600.4)
==25862== by 0x8416774: tvb_composite append (tvbuff_composite.c:223)
==25862== by 0x732E84A: decompress [z4 (packet-kafka.c:1372)
==25862== by 0x732E811: decompress (packet-kafka.c:1549)
==25862== by 0x732D9E5: dissect_kafka message old (packet-kafka.c:1763)
==25862== by 0x732D73C: dissect_kafka message (packet-kafka.c:1776)
==25862== by 0x732D5F5: dissect_kafka message set (packet-kafka.c:17797)
==25862== by 0x732D5F5: dissect_kafka message set (packet-kafka.c:1797)
==25862== by 0x732D5F5: dissect_kafka_produce_request_partition (packet-kafka.c:2973)
==25862== by 0x732D35F5: dissect_kafka_produce_request_partition (packet-kafka.c:2973)
   ...... at ux4C3OD3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==25862= by 0xD1C431: 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 0x840BCD51: tvb_free_internal (tvbuff.c:124)
==25862= by 0x840BCD5: tvb_free_chain (tvbuff.c:124)
==25862= by 0x840BCD5: tvb_free_shain (tvbuff.c:124)
==25862= by 0x127973: process_packet_single_pass_(tshark.c:3789)
==25862= by 0x127973: process_packet_single_pass_(tshark.c:3405)
by 0x127973: process_packet_single_pass_(tshark.c:3405)
==25862= by 0x1267C4: process_cap_file_tshark.c:3560)
==25862= by 0x1267C4: process_cap_file_tshark.c:3405
by 0x123CCb: main_(tshark.c:2044)
==25862= at 0x4C3OD3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux_so)
==25862= by 0xD1C431: g_slice_free_chain_with_offset_(in /usr/lib/valgrind/vgrulpilibglib-2.0.so.0.5600.4)
   linux.so)

by Outlic431: g slice free_chain_with_offset (in /usr/lib/x86_64-linux-qnu/libglib-2.0.so.0.5500.4)

==25862== by 0x841689s :composite_free (tvbuff_composite.c:41)

by 0x840Eb61: tvb_free_internal (tvbuff.c:19)

by 0x840Eb61: tvb_free_chain (tvbuff.c:124)

by 0x840Eb61: tvb_free_chain (tvbuff.c:124)

by 0x732Eb85: decompress [racket-kafka.c:1385)

==25862== by 0x732Eb85: dissect_kafka message old (packet-kafka.c:1776)

by 0x732D9E5: dissect_kafka message (packet-kafka.c:1777)

by 0x732D3E5Fs: dissect_kafka message (packet-kafka.c:1777)

==25862== by 0x732D3E5Fs: dissect_kafka message (packet-kafka.c:1777)

==25862== by 0x732D3E5Fs: dissect_kafka message (packet-kafka.c:1777)

==25862== by 0x732D48C: dissect_kafka message set (packet-kafka.c:1777)

==25862== by 0x732D48C: dissect_kafka message_set (packet-kafka.c:1777)
    ==25862== by UK/32U96: Gissett_marma_product_regression=0;

==25862= by UK732D395: dissett_kafka_array_ref (packet-kafka.c:907)

==25862= Block was alloc'd at

==25862= at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
       :=25862== by 0xDl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
-25862== by 0xDl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
        25862== by
.0.so.0.5600.4)
=25862==
                                                            OxD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
                                                             0xDllCEA3: g_slist_append (in /usr/lib/x86_64-linux-gnu/libglib-
        .0.so.0.5600.4)
=25862== h...
                                                0.4)
by 0x8416774: tvb_composite_append (tvbuff_composite.c:223)
by 0x732E84A: decompress_lz4 (packet-kafka.c:1372)
by 0x732E1C1: decompress (packet-kafka.c:1574)
by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
by 0x732D75E: dissect_kafka_message (packet-kafka.c:1797)
by 0x732D5FB: dissect_kafka_sessage stopacket-kafka.c:1797)
by 0x732D48C: dissect_kafka_produce_request_partition (packet-
    kafka.c:2973)
==25862==
                                                 by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
  ==25862= Invalid read of size 8
==25862= Invalid read of size 8
==25862= at 0x8416BA0: composite free (tvbuff composite.c:43)
==25862= by 0x840ECB0: tvb free Internal (tvbuff.c:39)
by 0x840ECB0: tvb free chain (tvbuff.c:124)
==25862= by 0x8395B87: epan dissect reset (epan.c:544)
by 0x127973: process packet single pass (tshark.c:3789)
==25862= by 0x1292ED: process cap file single pass (tshark.c:3405)
by 0x125CD: main (tshark.c:2044)
==25862= address 0x10bDfba0 is 64 bytes inside a block of size 80 free'd
==25862= at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
    linux.so)
==25862==
                                               by 0x840ED80: tvb_free_internal (tvbuff.c:103)
by 0x840EC80: tvb_free_chain (tvbuff.c:124)
by 0x73ZEB85: decompress 124 (packet-kafka.c:1385)
by 0x73ZED85: dissect_kafka.message_old (packet-kafka.c:1633)
by 0x73ZD73C: dissect_kafka_message_ (packet-kafka.c:1776)
by 0x73ZD57B: dissect_kafka_message_set (packet-kafka.c:1777)
by 0x73ZD57B: dissect_kafka_produce_request_partition (packet-
3)
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
     ==25862==
    kafka.c:2973)
==25862==
                                            by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
by 0x732D28D: dissect_kafka_produce_request_topic (packet-
     ==25862==
     ==25862==
   kafka.c:2994)
==25862== B1
==25862==
                                       Block was alloc'd at
   at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload memcheck-amd64-
    ==25862== by 0xDl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
   ==25862== by 0xDl1B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
  Invalid read of size 8
at 0x8416BAD: composite free (tvbuff composite.c:44)
by 0x840ED61: tvb free internal (tvbuff.c:99)
by 0x840ECE0: tvb free chain (tvbuff.c:124)
by 0x839B8F: epan dissect reset (epan.c:544)
by 0x127973: process packet single pass (tshark.c:3789)
by 0x129ZED: process cap file single pass (tshark.c:3405)
by 0x126TC4: process cap file (tshark.c:3560)
by 0x126TC0: main (tshark.c:2044)
Address 0x1b0bfba8 is 72 bytes inside a block of size 80 free'd
at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
       ==25862==
==25862==
==25862==
==25862==
==25862==
==25862==
==25862==
==25862==
==25862==
==25862==
   ==25862==
linux.so)
==25862==
==25862==
==25862==
==25862==
==25862==
                                                by 0x840ED80: tvb_free_internal (tvbuff.c:103)
by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
by 0x73ZEB85: decompress 124 (packet-kafka.c:1385)
by 0x73ZEIC1: decompress (packet-kafka.c:1549)
by 0x73ZD95: dissect_kafka message old (packet-kafka.c:1633)
by 0x73ZD73C: dissect_kafka_message (packet-kafka.c:1776)
```

```
==25862==
                                         by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797) by 0x732D48C: dissect_kafka_produce_request_partition (packet-
      =25862==
  kafka.c:2973)
                                          )
by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
by 0x732D28D: dissect_kafka_produce_request_topic (packet-
   ==25862==
   ==25862==
  kafka.c:2994)
                                   Block was alloc'd at
                                           at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload memcheck-amd64-
   ==25862==
 ==25862== by 0xDl03AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.soi.0.5600.4)
  ==25862== by 0xDllB955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
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 0x732ED5C: decompress 124 (packet-kafka.c:1308)
==25862== by 0x732E1C1: decompress (packet-kafka.c:1549)
==25862== by 0x732D73C: dissect_kafka_message old (packet-kafka.c:1633)
==25862== by 0x732D73C: dissect_kafka_message (packet-kafka.c:1776)
==25862== by 0x732D73C: dissect_kafka_message set (packet-kafka.c:1797)
==25862== by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
==25862== by 0x732D3EC: dissect_kafka_produce_request_partition (packet-kafka.c:2973)
by 0x732D3GS: dissect_kafka_produce_request_partition (packet-kafka.c:2973)
                                          by 0x732D395: dissect kafka array ref (packet-kafka.c:907)
 ==25862==
linux.so)
==25862== by 0x840ED80: tvb_free_internal (tvbuff.c:103)
==25862== by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
==25862== by 0x732EB85: decompress 124 (packet-kafka.c:1385)
==25862== by 0x732EIC1: decompress [cacket-kafka.c:1549]
==25862== by 0x732D95: dissect_kafka.message_old (packet-kafka.c:1776)
==25862== by 0x732D73C: dissect_kafka.message_old (packet-kafka.c:1776)
==25862== by 0x732D85: dissect_kafka.message_set (packet-kafka.c:1777)
by 0x732D48C: dissect_kafka.message_set (packet-kafka.c:1797)
==25862== by 0x732D85: dissect_kafka.produce_request_partition (packet-kafka.c:2973)
==25862= by 0x732D85: dissect_kafka.produce_request_partition (packet-kafka.c:2973)
                                          )
by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
by 0x732D28D: dissect_kafka_produce_request_topic (packet-
 Karka.c:2973)

by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862= by 0x732D1E4: dissect_kafka_array_ref (packet-kafka.c:923)
==25862= by 0x732D1E8: dissect_kafka_array_ref (packet-kafka.c:2923)
==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 0xD103AB8: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
    0.4)

by 0x840EBD7: tvb_new (tvbuff.c:75)

by 0x8416643: tvb_new composite (tvbuff_composite.c:197)

by 0x832E5D5: decompress 124 (packet-kafka.c:1308)

by 0x732E1C1: decompress (packet-kafka.c:1549)

by 0x732D95: dissect kafka message old (packet-kafka.c:1633)

by 0x732D73C: dissect kafka message (packet-kafka.c:1776)

by 0x732D5FB: dissect kafka message (packet-kafka.c:1797)

by 0x732D5FB: dissect kafka produce_request_partition (packet-
  kafka.c:2973)
==25862==
                                          by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
    =25862= Invalid read of size 8 at 0x8408D66: tvb free_internal (tvbuff.c:101) by 0x8408CEO: tvb free_chain (tvbuff.c:124) by 0x127973: process packet single pass (tshark.c:3789) ez5862= by 0x127973: process cap file single pass (tshark.c:3405) by 0x1267C4: process cap file single pass (tshark.c:3405) by 0x1267C4: process cap file (tshark.c:3560) by 0x1267C4: process cap file (tshark.c:3560) at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-alinux.so)
   ==25862==
                                                                                                                                                                                                                                                   -amd64-
      inux.so)
=25862==
                                       by 0x840ED80: tvb_free_internal (tvbuff.c:103)
by 0x840ECE0: tvb_free_chain (tvbuff.c:124)
by 0x732E85: decompress 124 (packet-kafka.c:1385)
by 0x732E85: decompress (packet-kafka.c:1549)
by 0x732D95: dissect kafka_message old (packet-kafka.c:1633)
by 0x732D73c: dissect_kafka_message (packet-kafka.c:1776)
by 0x732D5FB: dissect_kafka_message set (packet-kafka.c:1797)
by 0x732D58c: dissect_kafka_produce_request_partition (packet-
3)
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
 kafka.c:2973)
==25862==
==25862==
                                      by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
by 0x732D1E4: dissect_kafka_array (packet-kafka.c:923)
by 0x732D28D: dissect_kafka_produce_request_topic (packet-
   ==25862==
 kafka.c:2994)
==25862== B1
==25862==
                                  Block was alloc'd at
at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
  linux.so)
      =25862==
  ==25862== by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.5600.4)
      =25862==
                                                    OxD11B955: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
  ==25862== by
2.0.so.0.5600.4)
                                   by 0x840EBD7: tvb_new (tvbuff.c:75)
by 0x840EBD7: tvb_new (composite (tvbuff_composite.c:197)
by 0x8416643: tvb_new_composite (tvbuff_composite.c:197)
by 0x732E5D5: decompress [24 {packet-kafka.c:1308})
by 0x732EB1C1: decompress (packet-kafka.c:1549)
by 0x732D9E5: dissect_kafka_message_old (packet-kafka.c:1633)
by 0x732D7BC: dissect_kafka_message_set (packet-kafka.c:1776)
by 0x732D5FB: dissect_kafka_message_set (packet-kafka.c:1797)
by 0x732D48C: dissect_kafka_produce_request_partition (packet-73)
      =25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
  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==
==25862==
                                   by 0x840ED80: tvb free internal (tvbuff.c:103)
by 0x840ED80: tvb free chain (tvbuff.c:124)
by 0x839D8F: epan_dissect reset (epan.c:544)
by 0x127973: process packet single pass (tshark.c:3789)
by 0x1292ED: process cap file single pass (tshark.c:3405)
by 0x1267c4: process cap file (tshark.c:3560)
by 0x123CCD: main (tshark.c:2044)
Address 0x1bb0fb60 is 0 bytes inside a block of size 80 free'd
at 0x4C30D3B: free (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
   ==25862==
=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 0x73ZEBB: decompress 124 (packet-kafka.c:1385)
by 0x73ZEIC1: decompress (packet-kafka.c:1385)
by 0x73ZEIC1: decompress (packet-kafka.c:1549)
by 0x73ZEIC1: decompress (packet-kafka.c:1549)
by 0x73ZEIC1: decompress (packet-kafka.c:1797)
by 0x73ZD3D5E: dissect kafka message (packet-kafka.c:1777)
by 0x73ZD5FB: dissect kafka message (packet-kafka.c:1797)
by 0x73ZD5FB: dissect kafka produce request partition (packet-kafka.c:2737)
=25862= by 0x73ZD3D35: dissect kafka array_fe (packet-kafka.c:907)
=25862= by 0x73ZD3D35: dissect kafka array_fe (packet-kafka.c:923)
by 0x73ZD2B1: dissect kafka_raray_fe (packet-kafka.c:923)
=25862= by 0x73ZD2B1: dissect_kafka_raray_fe (packet-kafka.c:923)
=25862= by 0x73ZD2B1: dissect_kafka_produce_request_partition (packet-kafka.c:2994)
=25862= Block was alloc'd at
=25862= at 0x4C2FB0F: malloc (in /usr/lib/vaff.fb.lieuv.gm/(lib/dib.
     =25862==
  linux.so)
==25862==
                                          by 0xD103AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
```

```
2.0.so.0.5600.4)
==25862== by (0x810BBD7: tvb new (tvbuff.c:75)
==25862== by (0x840BBD7: tvb new (tvbuff.c:75)
==25862== by (0x8416632: tvb new composite (tvbuff composite.c:197)
==25862== by (0x732E5D5: decompress [r4 (packet-kafka.c:1308)
==25862== by 0x732E5D5: decompress [packet-kafka.c:154]
==25862== by 0x732DB5: dissect kafka message old (packet-kafka.c:1633)
==25862== by 0x732DB5: dissect kafka message old (packet-kafka.c:1776)
==25862== by 0x732D3D5B2: dissect kafka message (packet-kafka.c:1777)
==25862== by 0x732D5B2: dissect kafka message (packet-kafka.c:1777)
==25862== by 0x732D5B2: dissect kafka produce_request_partition (packet-kafka.c:2973)
==25862== by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862== by 0x732D395: dissect_kafka_array_ref (packet-kafka.c:907)
==25862== total packet for the packet for the
   2.0.so.0.5600.4)
      ==25862== total heap usage: 330,264 allocs, 330,063 frees, 40,608,136 bytallocated
==25862== LEAK SUMMARY:
==25862== indirectly lost: 0 bytes in 0 blocks
==25862== possibly lost: 304 bytes in 1 blocks
==25862== suppressed: 803 bytes in 33 blocks
==25862== suppressed: 803 bytes in 33 blocks
==25862== Ferous with --leak-check=full to see details of leaked memory
==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: 1z4: 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: 1z4: free the composite tvb only once

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