Bug 16341 - [oss-fuzz] Indirect-leak in dissect_lte_rrc_SystemInfoListGERAN_item

Status: RESOLVED FIXED

Alias: None

Product: Wireshark
Component: Dissection engine (libwireshark) (show other bugs)
Version: Git
Hardware: x86-64 Linux

Importance: Low Major (vote)
Target Milestone: ---
Assignee: Bugzilla Administrator

URL: https://bugs.chromium.org/p/oss-fuzz/...

Depends on:
Blocks:

Reported: 2020-01-21 18:28 UTC by Gerald Combs
Modified: 2020-04-10 15:34 UTC (History)
CC List: 2 users (show)

See Also: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9431

Attachments	
Reproducer testcase (115 bytes, application/octet-stream) 2020-01-21 18:28 UTC, Gerald Combs	Details
Add an attachment (proposed patch, testcase, etc.)	

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

Gerald Combs 2020-01-21 18:28:17 UTC **Description**

```
Created attachment 17581 [details]
Reproducer testcase

Build Information:
Paste the COMPLETE build information from "Help->About Wireshark", "wireshark -v",
or "tshark -v".
--
OSS-Fuzz found an issue in the LTE RRC dissector:

[Environment]
ASAN_OPTIONS="alloc_dealloc_mismatch=0:allocator_may_return_null=1:allocator_release_to_os_interval_ms=500:allow_user_segv_handler=0:check_malloc_usable_size=0:detect_leaks=1:detect_odr_violation=0:detect_stack_use_after_return=1:fast_unwind_on_fatal=0:handle_abort=1:
        +-----------------------------------------Release Build Stacktrace----------
------------------------------+
        oss-fuzzshark: disabling: ip
        oss-fuzzshark: disabling: udplite
        oss-fuzzshark: disabling: ospf
        oss-fuzzshark: disabling: bgp
        oss-fuzzshark: disabling: dhcp
        oss-fuzzshark: disabling: json
        oss-fuzzshark: disabling: snort
        oss-fuzzshark: configured for dissector: udp in table: ip.proto
        INFO: Seed: 1120630464
        INFO: Loaded 1 modules   (352024 inline 8-bit counters): 352024 [0xde25fb0,
0xde7bec8),
        INFO: Loaded 1 PC tables (352024 PCs): 352024 [0xde7bec8,0xe3db048),
        INFO: -fork=1: fuzzing in separate process(s)
        INFO: -fork=1: 1517 seed inputs, starting to fuzz in
/tmp/libFuzzerTemp.1.dir
        #77: cov: 19646 ft: 32270 corp: 1517 exec/s 15 oom/timeout/crash: 0/0/0
time: 13s job: 1 dft_time: 0
        #136: cov: 19646 ft: 32270 corp: 1517 exec/s 14 oom/timeout/crash: 0/0/0
time: 18s job: 2 dft_time: 0
        INFO: log from the inner process:
        oss-fuzzshark: disabling: ip
        oss-fuzzshark: disabling: udplite
        oss-fuzzshark: disabling: ospf
        oss-fuzzshark: disabling: bgp
        oss-fuzzshark: disabling: dhcp
        oss-fuzzshark: disabling: json
        oss-fuzzshark: disabling: snort
        oss-fuzzshark: configured for dissector: udp in table: ip.proto
        INFO: Seed: 1134549287
        INFO: Loaded 1 modules   (352024 inline 8-bit counters): 352024 [0xde25fb0,
0xde7bec8),
        INFO: Loaded 1 PC tables (352024 PCs): 352024 [0xde7bec8,0xe3db048),
        INFO:        0 files found in /tmp/libFuzzerTemp.1.dir/C2
        INFO: seed corpus: files: 38 min: 28b max: 359b total: 3905b rss: 274Mb
        #32  pulse  cov: 1555 ft: 2390 corp: 15/901b exec/s: 16 rss: 306Mb

        =================================================================
        ==63==ERROR: LeakSanitizer: detected memory leaks

        Indirect leak of 160 byte(s) in 2 object(s) allocated from:
            #0 0x523ecd in __interceptor_malloc /src/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145:3
            #1 0x2815b48 in g_malloc
            #2 0x2737559 in tvb_new_composite
/src/wireshark/epan/tvbuff_composite.c:198:18
            #3 0x226956a in dissect_lte_rrc_SystemInfoListGERAN_item
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:51773:39
            #4 0x17719e4 in dissect_per_sequence_of_helper
/src/wireshark/epan/dissectors/packet-per.c:568:10
            #5 0x17719e4 in dissect_per_constrained_sequence_of
/src/wireshark/epan/dissectors/packet-per.c:943:9
            #6 0x226931b in dissect_lte_rrc_SystemInfoListGERAN
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:51799:12
            #7 0x226931b in dissect_lte_rrc_T_psi /work/build/asn1/lte-rrc/packet-
lte-rrc-fn.c:51823:12
            #8 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #9 0x2269141 in dissect_lte_rrc_SI_OrPSI_GERAN /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51845:12
            #10 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #11 0x22686c8 in dissect_lte_rrc_Handover /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51865:12
            #12 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #13 0x22685b1 in dissect_lte_rrc_T_purpose /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51977:12
            #14 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #15 0x2268536 in dissect_lte_rrc_MobilityFromEUTRACommand_r8_IEs
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52037:12
            #16 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #17 0x22684b1 in dissect_lte_rrc_T_c1_26 /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:52193:12
            #18 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #19 0x2268471 in dissect_lte_rrc_T_criticalExtensions_20
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52228:12
            #20 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #21 0x226762b in dissect_lte_rrc_MobilityFromEUTRACommand
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52247:12
            #22 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #23 0x2267301 in dissect_lte_rrc_T_c1_13 /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:56723:12
            #24 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #25 0x22672c1 in dissect_lte_rrc_DL_DCCH_MessageType
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:56758:12
            #26 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #27 0x2200e73 in dissect_lte_rrc_DL_DCCH_Message /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:56775:12
            #28 0x2200e73 in dissect_DL_DCCH_Message_PDU /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:97026:12
            #29 0x2200e73 in dissect_lte_rrc_DL_DCCH /work/build/asn1/lte-
rrc/packet-lte-rrc-template.c:3209:3
            #30 0x6d3a22 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #31 0x6d3a22 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #32 0x6d038b in call_dissector_only /src/wireshark/epan/packet.c:3208:8
            #33 0x6d038b in call_dissector_with_data
/src/wireshark/epan/packet.c:3221:8
            #34 0x111b017 in dissect_gsmtap /src/wireshark/epan/dissectors/packet-
gsmtap.c:0
            #35 0x6d3a22 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #36 0x6d3a22 in call_dissector_work /src/wireshark/epan/packet.c:799:9

        Indirect leak of 128 byte(s) in 2 object(s) allocated from:
            #0 0x523ecd in __interceptor_malloc /src/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145:3
            #1 0x2815b48 in g_malloc
            #2 0x7dc4e1 in tvb_new_real_data /src/wireshark/epan/tvbuff_real.c:65:8
            #3 0x22695e1 in dissect_lte_rrc_SystemInfoListGERAN_item
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:51776:49
            #4 0x17719e4 in dissect_per_sequence_of_helper
/src/wireshark/epan/dissectors/packet-per.c:568:10
            #5 0x17719e4 in dissect_per_constrained_sequence_of
/src/wireshark/epan/dissectors/packet-per.c:943:9
            #6 0x226931b in dissect_lte_rrc_SystemInfoListGERAN
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:51799:12
            #7 0x226931b in dissect_lte_rrc_T_psi /work/build/asn1/lte-rrc/packet-
lte-rrc-fn.c:51823:12
            #8 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #9 0x2269141 in dissect_lte_rrc_SI_OrPSI_GERAN /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51845:12
            #10 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #11 0x22686c8 in dissect_lte_rrc_Handover /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51865:12
            #12 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #13 0x22685b1 in dissect_lte_rrc_T_purpose /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51977:12
            #14 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #15 0x2268536 in dissect_lte_rrc_MobilityFromEUTRACommand_r8_IEs
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52037:12
            #16 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #17 0x22684b1 in dissect_lte_rrc_T_c1_26 /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:52193:12
            #18 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #19 0x2268471 in dissect_lte_rrc_T_criticalExtensions_20
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52228:12
            #20 0x1777e93 in dissect_per_sequence
```

```
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #21 0x226762b in dissect_lte_rrc_MobilityFromEUTRACommand
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52247:12
            #22 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #23 0x2267301 in dissect_lte_rrc_T_c1_13 /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:56723:12
            #24 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #25 0x22672c1 in dissect_lte_rrc_DL_DCCH_MessageType
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:56758:12
            #26 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #27 0x2200e73 in dissect_lte_rrc_DL_DCCH_Message /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:56775:12
            #28 0x2200e73 in dissect_DL_DCCH_Message_PDU /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:97026:12
            #29 0x2200e73 in dissect_lte_rrc_DL_DCCH /work/build/asn1/lte-
rrc/packet-lte-rrc-template.c:3209:3
            #30 0x6d3a22 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #31 0x6d3a22 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #32 0x6d038b in call_dissector_only /src/wireshark/epan/packet.c:3208:8
            #33 0x6d038b in call_dissector_with_data
/src/wireshark/epan/packet.c:3221:8
            #34 0x111b017 in dissect_gsmtap /src/wireshark/epan/dissectors/packet-
gsmtap.c:0
            #35 0x6d3a22 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #36 0x6d3a22 in call_dissector_work /src/wireshark/epan/packet.c:799:9

        Indirect leak of 64 byte(s) in 4 object(s) allocated from:
            #0 0x523ecd in __interceptor_malloc /src/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145:3
            #1 0x2815b48 in g_malloc

        Indirect leak of 32 byte(s) in 4 object(s) allocated from:
            #0 0x523ecd in __interceptor_malloc /src/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145:3
            #1 0x2815b48 in g_malloc
            #2 0x2269611 in dissect_lte_rrc_SystemInfoListGERAN_item
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:51778:9
            #3 0x17719e4 in dissect_per_sequence_of_helper
/src/wireshark/epan/dissectors/packet-per.c:568:10
            #4 0x17719e4 in dissect_per_constrained_sequence_of
/src/wireshark/epan/dissectors/packet-per.c:943:9
            #5 0x226931b in dissect_lte_rrc_SystemInfoListGERAN
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:51799:12
            #6 0x226931b in dissect_lte_rrc_T_psi /work/build/asn1/lte-rrc/packet-
lte-rrc-fn.c:51823:12
            #7 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #8 0x2269141 in dissect_lte_rrc_SI_OrPSI_GERAN /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51845:12
            #9 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #10 0x22686c8 in dissect_lte_rrc_Handover /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51865:12
            #11 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #12 0x22685b1 in dissect_lte_rrc_T_purpose /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:51977:12
            #13 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #14 0x2268536 in dissect_lte_rrc_MobilityFromEUTRACommand_r8_IEs
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52037:12
            #15 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #16 0x22684b1 in dissect_lte_rrc_T_c1_26 /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:52193:12
            #17 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #18 0x2268471 in dissect_lte_rrc_T_criticalExtensions_20
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52228:12
            #19 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #20 0x226762b in dissect_lte_rrc_MobilityFromEUTRACommand
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:52247:12
            #21 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #22 0x2267301 in dissect_lte_rrc_T_c1_13 /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:56723:12
            #23 0x1777182 in dissect_per_choice
/src/wireshark/epan/dissectors/packet-per.c:1751:13
            #24 0x22672c1 in dissect_lte_rrc_DL_DCCH_MessageType
/work/build/asn1/lte-rrc/packet-lte-rrc-fn.c:56758:12
            #25 0x1777e93 in dissect_per_sequence
/src/wireshark/epan/dissectors/packet-per.c:1908:12
            #26 0x2200e73 in dissect_lte_rrc_DL_DCCH_Message /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:56775:12
            #27 0x2200e73 in dissect_DL_DCCH_Message_PDU /work/build/asn1/lte-
rrc/packet-lte-rrc-fn.c:97026:12
            #28 0x2200e73 in dissect_lte_rrc_DL_DCCH /work/build/asn1/lte-
rrc/packet-lte-rrc-template.c:3209:3
            #29 0x6d3a22 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #30 0x6d3a22 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #31 0x6d038b in call_dissector_only /src/wireshark/epan/packet.c:3208:8
            #32 0x6d038b in call_dissector_with_data
/src/wireshark/epan/packet.c:3221:8
            #33 0x111b017 in dissect_gsmtap /src/wireshark/epan/dissectors/packet-
gsmtap.c:0
            #34 0x6d3a22 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #35 0x6d3a22 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #36 0x6d3f96 in dissector_try_uint_new
/src/wireshark/epan/packet.c:1399:8
            #37 0x6d3f96 in dissector_try_uint /src/wireshark/epan/packet.c:1423:9

        SUMMARY: AddressSanitizer: 384 byte(s) leaked in 12 allocation(s).

        INFO: a leak has been found in the initial corpus.

        INFO: to ignore leaks on libFuzzer side use -detect_leaks=0.

        MS: 0 ; base unit: 0000000000000000000000000000000000000000

0x12,0x79,0x52,0xc,0x3d,0x3d,0x3,0x50,0xc5,0xc1,0xd,0x24,0x1a,0x12,0x8b,0x28,0x30,0x89,0x4,0x61,0x1,0xf9,0xb1,0x26,0x30,0x89,0xfc,0x60,0x1,0x1b,0xb0,0x2e,0xa6,0xb3,0xf9,0xb1,0x26,0x30,0x75,0xb8,0xff,0x4a,0xdb,0x0,0x0,0x0,0x60,0x1,0x1b,0xb0,0x2e,0xa6,0xb3,0xf9,0xb1,0x2

\x12yR\x0c==\x03P\xc5\xc1\x0d$\x1a\x12\x8b(0\x89\x04a\x01\xf9\xb1&0\x89\xfc`\x01\x1b\xb0.\xa6\xb3\xf9\xb1&0u\xb8\xffJ\xdb\x00\x00\x00`\x01\x1b\xb0.\xa6\xb3\xf9\xb1&32769\x89\xfc`\x01\x1b\xb0.\xa6\xb3\xf9\xb1&0u\xb8\xffJ\xdb\x00\x00\x00`\x01\x1b\xb0.\xa6\xb3\xf9\xb1&31
        artifact_prefix='/fuzzer-testcases/'; Test unit written to /fuzzer-
testcases/leak-bc9f30f7f07d98077e20b40dacd887b0d612a392
        Base64:
EnlSDD09A1DFwQ0kGhKLKDCJBGEB+bEmMIn8YAEbsC6ms/mxJjB1uP9K2wAAAGABG7AuprP5sSYzMjc2OYn8YAEbsC6ms/mxJjB1uP9K2wAAAGABG7AuprP5sSYzMYlHALUk////W9f/AAASO+EBVP8AAg==
        stat::number_of_executed_units: 59
        stat::average_exec_per_sec:     14
        stat::new_units_added:          0
        stat::slowest_unit_time_sec:    0
        stat::peak_rss_mb:              308
        INFO: exiting: 77 time: 18s
```

Pascal Quantin 2020-01-21 18:32:40 UTC Comment 1

I will have a look at it tonight.

Pascal Quantin 2020-01-21 21:31:10 UTC Comment 2

Could one remind me how we are supposed to use the reproducer testcase?
I tried running fuzzshark_ip_proto_udp clusterXXX but it does not seem to work and
I do not remember how I did last time (a few months back...)

Pascal Quantin 2020-01-21 22:01:53 UTC Comment 3

I generated a pcap from the test case using
https://github.com/Lekensteyn/wireshark-fuzztools but ASAN/UBSan does not report
any leak when compiling master branch with Clang (even when using the ASAN_OPTIONS
provided in the bug report).
Can anyone else reproduce it?

Gerald Combs 2020-01-22 01:28:04 UTC Comment 4

(In reply to Pascal Quantin from comment #3)
> I generated a pcap from the test case using
> https://github.com/Lekensteyn/wireshark-fuzztools but ASAN/UBSan does not
> report any leak when compiling master branch with Clang (even when using the
> ASAN_OPTIONS provided in the bug report).
> Can anyone else reproduce it?

I wasn't able to reproduce it using ASAN, but I was able to using Valgrind:

```
FUZZSHARK_TARGET=udp valgrind --tool=memcheck --leak-check=full ./run/fuzzshark
/tmp/clusterfuzz-testcase-fuzzshark_ip_proto-udp-5717949700898816

==24884== Memcheck, a memory error detector
==24884== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==24884== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==24884== Command: ./run/fuzzshark /tmp/clusterfuzz-testcase-fuzzshark_ip_proto-
udp-5717949700898816
==24884==
StandaloneFuzzTargetMain: running 1 inputs
oss-fuzzshark: disabling: snort
oss-fuzzshark: requested dissector: udp
Running: /tmp/clusterfuzz-testcase-fuzzshark_ip_proto-udp-5717949700898816
Done:    /tmp/clusterfuzz-testcase-fuzzshark_ip_proto-udp-5717949700898816: (115
bytes)
==24884==
==24884== HEAP SUMMARY:
==24884==     in use at exit: 26,144,108 bytes in 274,854 blocks
==24884==   total heap usage: 314,832 allocs, 39,978 frees, 39,860,604 bytes
allocated
==24884==
==24884== 384 (160 direct, 224 indirect) bytes in 2 blocks are definitely lost in
loss record 55,275 of 56,741
==24884==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==24884==    by 0xC1DAAB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==24884==    by 0xC1F2975: g_slice_alloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==24884==    by 0x7A367F4: tvb_new (tvbuff.c:75)
==24884==    by 0x7A403AF: tvb_new_composite (tvbuff_composite.c:198)
==24884==    by 0x776B09D: dissect_lte_rrc_SystemInfoListGERAN_item (packet-lte-
rrc-fn.c:51773)
==24884==    by 0x727D597: dissect_per_sequence_of_helper (packet-per.c:568)
==24884==    by 0x7280124: dissect_per_constrained_sequence_of (packet-per.c:943)
==24884==    by 0x776A741: dissect_lte_rrc_SystemInfoListGERAN (packet-lte-rrc-
fn.c:51799)
==24884==    by 0x776A741: dissect_lte_rrc_T_psi (packet-lte-rrc-fn.c:51823)
==24884==    by 0x7281345: dissect_per_choice (packet-per.c:1751)
==24884==    by 0x774D9F9: dissect_lte_rrc_SI_OrPSI_GERAN (packet-lte-rrc-
fn.c:51845)
==24884==    by 0x728171E: dissect_per_sequence (packet-per.c:1908)
==24884==
==24884== LEAK SUMMARY:
==24884==    definitely lost: 160 bytes in 2 blocks
==24884==    indirectly lost: 224 bytes in 10 blocks
==24884==      possibly lost: 0 bytes in 0 blocks
==24884==    still reachable: 26,143,724 bytes in 274,842 blocks
==24884==         suppressed: 0 bytes in 0 blocks
==24884== Reachable blocks (those to which a pointer was found) are not shown.
==24884== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==24884==
==24884== For counts of detected and suppressed errors, rerun with: -v
==24884== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

Where are we freeing si_tvb and gsm_rlcmac_dl_tvb in dissect_lte_rrc_SystemInfoListGERAN_item?

Pascal Quantin 2020-01-22 10:08:48 UTC Comment 5

I thought composite TVBs were added automatically to the tvb chain, but indeed this is not the case. Stupid mistake.

Gerrit Code Review 2020-01-22 10:43:07 UTC Comment 6

Change 35899 had a related patch set uploaded by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35899

Gerrit Code Review 2020-01-22 11:26:14 UTC Comment 7

Change 35899 merged by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35899

Gerrit Code Review 2020-01-22 11:26:44 UTC Comment 8

Change 35901 had a related patch set uploaded by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35901

Gerrit Code Review 2020-01-22 11:27:09 UTC Comment 9

Change 35901 merged by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35901

Gerrit Code Review 2020-01-22 11:27:22 UTC Comment 10

Change 35902 had a related patch set uploaded by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35902

Gerrit Code Review 2020-01-22 11:27:45 UTC Comment 11

Change 35902 merged by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35902

Gerrit Code Review 2020-01-22 11:44:29 UTC Comment 12

Change 35903 had a related patch set uploaded by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35903

Gerrit Code Review 2020-01-22 11:49:41 UTC Comment 13

Change 35903 merged by Pascal Quantin:
LTE RRC: fix a memory leak in composite TVB handling

https://code.wireshark.org/review/35903

Format For Printing - XML - Clone This Bug - Top of page