Closed Issue created 2 years ago by Wireshark GitLab Migration

Buildbot crash output: fuzz-2020-07-28-5905.pcap

This issue was migrated from bug 16741 in our old bug tracker.

Original bug information:

Reporter: Buildbot Builder
Status: CONFIRMED
Product: Wireshark
Component: Dissection engine (libwireshark)
OS: Ubuntu
Platform: x86-64
Version: unspecified

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Related merge requests 4

multipart: fix deallocation of invalid parts
!96

multipart: fix deallocation of invalid parts
!98

multipart: fix deallocation of invalid parts
!99

multipart: fix deallocation of invalid parts
!100

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

Activity

Wireshark GitLab Migration @ws-gitlab-migration · 2 years ago Author

Buildbot Builder said:

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

https://www.wireshark.org/download/automated/captures/fuzz-2020-07-28-5905.pcap

stderr:
Input file: /home/wireshark/menagerie/menagerie/14213-servermanager_test.pcapng

Build host information:
Linux build6 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 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=fuzz-test
BUILDBOT_BUILDNUMBER=211
BUILDBOT_BUILDERNAME=Fuzz Test
BUILDBOT_URL=http://buildbot.wireshark.org/wireshark-3.0/
BUILDBOT_REPOSITORY=ssh://wireshark-buildbot@code.wireshark.org:29418/wireshark
BUILDBOT_GOT_REVISION=97c3ed7878a37a0ebaf6bc11f8ac32d2bde6a079

Return value:  0

Dissector bug:  0

Valgrind error count:  0



Git commit
commit 97c3ed7878a37a0ebaf6bc11f8ac32d2bde6a079
Author: Jaap Keuter <jaap.keuter@xs4all.nl>
Date:   Sun Jul 26 11:17:38 2020 +0200

    MQ: Fix short NameValue presentation

    Patch from Robert Grange

    Bug: 16733
    Change-Id: I7a11e060bb89aa1279a212f9dd958931c1031846
    Reviewed-on: https://code.wireshark.org/review/37967
    Reviewed-by: Jaap Keuter <jaap.keuter@xs4all.nl>
    Petri-Dish: Jaap Keuter <jaap.keuter@xs4all.nl>
    Tested-by: Petri Dish Buildbot
    Reviewed-by: Anders Broman <a.broman58@gmail.com>
    (cherry picked from commit dba5465f1173bcb5992854e74b610aaef14a4989)
    Reviewed-on: https://code.wireshark.org/review/37969


Command and args: /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/install.asan/bin/tshark  -nVxr
=================================================================
==6884==ERROR: AddressSanitizer: attempting free on address which was not malloc()-ed: 0x61b00004bba0 in thread T
    #0 0x5574ac921ec2 in __interceptor_free (/home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/install.asan/bi
    #1 0x7f5ad268c0b3 in get_multipart_info /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/..
    #2 0x7f5ad268b741 in dissect_multipart /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #3 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build
    #4 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #5 0x7f5ad44280f0 in call_dissector_only /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #6 0x7f5ad21119cb in dissect_http_message /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #7 0x7f5ad210b3c2 in dissect_http_on_stream /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuil
    #8 0x7f5ad2107933 in dissect_http_tcp /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../e
    #9 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build
    #10 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #11 0x7f5ad4420653 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #12 0x7f5ad2f365cf in decode_tcp_ports /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #13 0x7f5ad2f3d1a9 in process_tcp_payload /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #14 0x7f5ad2f49229 in dissect_tcp /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epan/
    #15 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #16 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #17 0x7f5ad4420653 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #18 0x7f5ad22565f2 in ip_try_dissect /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../ep
    #19 0x7f5ad225d5e3 in dissect_ip_v4 /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epa
    #20 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #21 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #22 0x7f5ad4420653 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #23 0x7f5ad44210fb in dissector_try_uint /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #24 0x7f5ad1e123f0 in dissect_ethertype /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/..
    #25 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #26 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #27 0x7f5ad44280f0 in call_dissector_only /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #28 0x7f5ad441cf74 in call_dissector_with_data /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmb
    #29 0x7f5ad1e0fad6 in dissect_eth_common /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #30 0x7f5ad1e0b513 in dissect_eth /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epan/
    #31 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #32 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #33 0x7f5ad44280f0 in call_dissector_only /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #34 0x7f5ad1ecb6ce in dissect_frame /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epa
    #35 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #36 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #37 0x7f5ad44280f0 in call_dissector_only /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #38 0x7f5ad441cf74 in call_dissector_with_data /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmb
    #39 0x7f5ad441c776 in dissect_record /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../ep
    #40 0x7f5ad43ec848 in epan_dissect_run_with_taps /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/c
    #41 0x5574ac9821f0 in process_packet_single_pass /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/c
    #42 0x5574ac97e139 in process_cap_file /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #43 0x5574ac978cc3 in main /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../tshark.c:203
    #44 0x7f5ac6c62b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
    #45 0x5574ac876879 in _start (/home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/install.asan/bin/tshark+0x

0x61b00004bba0 is located 32 bytes inside of 1411-byte region [0x61b00004bb80,0x61b00004c103)
allocated by thread T0 here:
    #0 0x5574ac922243 in __interceptor_malloc (/home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/install.asan/
    #1 0x7f5ac76c2ab8 in g_malloc (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x51ab8)
    #2 0x7f5ad4307162 in wmem_strict_alloc /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #3 0x7f5ad42fdbd9 in wmem_alloc /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epan/wm
    #4 0x7f5ad440c3c7 in ws_find_media_type_parameter /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/
    #5 0x7f5ad268c027 in get_multipart_info /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/..
    #6 0x7f5ad268b741 in dissect_multipart /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #7 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build
    #8 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #9 0x7f5ad44280f0 in call_dissector_only /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #10 0x7f5ad21119cb in dissect_http_message /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild
    #11 0x7f5ad210b3c2 in dissect_http_on_stream /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #12 0x7f5ad2107933 in dissect_http_tcp /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #13 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #14 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #15 0x7f5ad4420653 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #16 0x7f5ad2f365cf in decode_tcp_ports /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../
    #17 0x7f5ad2f3d1a9 in process_tcp_payload /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #18 0x7f5ad2f49229 in dissect_tcp /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epan/
    #19 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #20 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #21 0x7f5ad4420653 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #22 0x7f5ad22565f2 in ip_try_dissect /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../ep
    #23 0x7f5ad225d5e3 in dissect_ip_v4 /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/../epa
    #24 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil
    #25 0x7f5ad4420d29 in call_dissector_work /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/
    #26 0x7f5ad4420653 in dissector_try_uint_new /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbui
    #27 0x7f5ad44210fb in dissector_try_uint /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/.
    #28 0x7f5ad1e123f0 in dissect_ethertype /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/build/cmbuild/..
    #29 0x7f5ad442b844 in call_dissector_through_handle /home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/buil

SUMMARY: AddressSanitizer: bad-free (/home/wireshark/builders/wireshark-3.0-fuzz/fuzztest/install.asan/bin/tshark
==6884==ABORTING

[ no debug trace ]
```

Wireshark GitLab Migration added crash label 2 years ago

Wireshark GitLab Migration added lib wireshark os ubuntu scoped labels 2 years ago

George Hopkins mentioned in merge request !96 (merged) 2 years ago

Pascal Quantin closed via merge request !96 (merged) 2 years ago

George Hopkins mentioned in commit 21f082cb 2 years ago

Pascal Quantin mentioned in merge request !98 (merged) 2 years ago

George Hopkins mentioned in commit 14e274f3 2 years ago

Pascal Quantin mentioned in merge request !99 (merged) 2 years ago

George Hopkins mentioned in commit 5803c7b8 2 years ago

Pascal Quantin mentioned in merge request !100 (merged) 2 years ago

Gerald Combs @geraldcombs · 2 years ago Owner

CVE-2020-25863

Edited by Gerald Combs 2 years ago

Please register or sign in to reply