Closed · Issue created 2 years ago by Wireshark GitLab Migration

Buildbot crash output: fuzz-2020-07-28-14741.pcap

This issue was migrated from bug 16739 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 3

Kafka: Limit our decompression size.
!1100

Kafka: Limit our decompression size.
!1108

Kafka: Limit our decompression size.
!1165

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-2020-07-28-14741.pcap

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

Build host information:
Linux build6 4.15.0-111-generic #112-Ubuntu SMP Thu Jul 9 20:32:34 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=5270
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=6b400e27afbcef46e1c6c6b583e829b6fd66328b

Return value:  0

Dissector bug:  0

Valgrind error count:  0



Git commit
commit 6b400e27afbcef46e1c6c6b583e829b6fd66328b
Author: Tomasz Moń <desowin@gmail.com>
Date:   Sat Jul 25 13:41:36 2020 +0200

    FTDI MPSSE: Link Bad Command when skipping data

    Show the Bad Command code and from which packet it originates from when
    skipping data while searching for Bad Command response.

    Ping-Bug: 11743
    Change-Id: I3b500a5e9f780775dfad9ce03cff911a6c1e2c41
    Reviewed-on: https://code.wireshark.org/review/37954
    Petri-Dish: Tomasz Moń <desowin@gmail.com>
    Tested-by: Petri Dish Buildbot
    Reviewed-by: Anders Broman <a.broman58@gmail.com>


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

** (process:19742): WARNING **: 12:34:01.859: Dissector bug, protocol Kafka, in packet 31: ../epan/proto.c:4272:
AddressSanitizer:DEADLYSIGNAL
=================================================================
==19742==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f2b68871561 bp 0x7ffd8c4bca10 sp
==19742==The signal is caused by a READ memory access.
==19742==Hint: address points to the zero page.
    #0 0x7f2b68871560 in value_get /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build/cmbuild
    #1 0x7f2b6886ef23 in fvalue_get /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build/cmbuil
    #2 0x7f2b68a4d2c8 in proto_item_fill_label /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/b
    #3 0x7f2b689c68bf in proto_tree_print_node /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/b
    #4 0x7f2b68a07557 in proto_tree_children_foreach /home/wireshark/builders/wireshark-master-fuzz/clangcodeanal
    #5 0x7f2b689c739c in proto_tree_print_node /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/b
    #6 0x7f2b68a07557 in proto_tree_children_foreach /home/wireshark/builders/wireshark-master-fuzz/clangcodeanal
    #7 0x7f2b689c739c in proto_tree_print_node /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/b
    #8 0x7f2b68a07557 in proto_tree_children_foreach /home/wireshark/builders/wireshark-master-fuzz/clangcodeanal
    #9 0x7f2b689c739c in proto_tree_print_node /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/b
    #10 0x7f2b68a07557 in proto_tree_children_foreach /home/wireshark/builders/wireshark-master-fuzz/clangcodeana
    #11 0x7f2b689c739c in proto_tree_print_node /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/
    #12 0x7f2b68a07557 in proto_tree_children_foreach /home/wireshark/builders/wireshark-master-fuzz/clangcodeana
    #13 0x7f2b689c739c in proto_tree_print_node /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/
    #14 0x7f2b68a07557 in proto_tree_children_foreach /home/wireshark/builders/wireshark-master-fuzz/clangcodeana
    #15 0x7f2b689c6425 in proto_tree_print /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build
    #16 0x55776be54773 in print_packet /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build/cmb
    #17 0x55776be54412 in process_packet_single_pass /home/wireshark/builders/wireshark-master-fuzz/clangcodeanal
    #18 0x55776be57b97 in process_cap_file_single_pass /home/wireshark/builders/wireshark-master-fuzz/clangcodear
    #19 0x55776be5162c in process_cap_file /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build
    #20 0x55776be4b341 in main /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build/cmbuild/../
    #21 0x7f2b5a967b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
    #22 0x55776bd47cd9 in _start (/home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/install.asan/b

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/wireshark/builders/wireshark-master-fuzz/clangcodeanalysis/build/cmbuild/..
==19742==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

Gerald Combs mentioned in merge request !1100 (merged) 2 years ago

A Wireshark GitLab Utility closed via merge request !1100 (merged) 2 years ago

Gerald Combs mentioned in commit fa537254 2 years ago

Gerald Combs mentioned in merge request !1108 (merged) 2 years ago

Gerald Combs mentioned in merge request !1165 (merged) 2 years ago

Gerald Combs made the issue confidential 2 years ago

Gerald Combs made the issue visible to everyone 2 years ago

Gerald Combs @geraldcombs · 2 years ago Owner

This also triggered

```
    ** (process:17681): WARNING **: 20:03:07.440: Dissector bug, protocol Kafka, in packet 31: ../epan/proto.c:70
```

which is what MRs !1100 (merged), !1108 (merged), and !1165 (merged) fix.

Gerald Combs mentioned in commit 4736aaae 1 year ago

Please register or sign in to reply