

Buildbot crash output: fuzz-2021-10-23-10702.pcap

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2021-10-23-10702.pcap>

stderr:

```
Input file: /var/menagerie/menagerie/2566-omni.out.2.hdlc.pcap

Build host information:
Linux runner-yq5rvme-project-7898047-concurrent-1 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:58:18 UTC 2021 x86_64 x86_64
Distributor ID: Ubuntu
Description: Ubuntu 20.04.3 LTS
Release: 20.04
Codename: focal

Return value: 0

Dissector bug: 0

Valgrind error count: 1

Latest (but not necessarily the problem) commit:
ca8e6f3d Qt: Add back some Q_OBJECT calls.

Command and args: ./tools/valgrind-wireshark.sh -b /builds/wireshark/wireshark/_install/bin
==24061== Memcheck, a memory error detector
==24061== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==24061== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info
==24061== Command: /builds/wireshark/wireshark/_install/bin/tshark -nr /tmp/fuzz/fuzz-2021-10-23-10702.pcap
==24061==
Running as user "root" and group "root". This could be dangerous.
==24061== Warning: set address range perms: large range [0xd2c9e028, 0xa2c9e058] (noaccess)
==24061==
==24061== Process terminating with default action of signal 24 (SIGXCPU): dumping core
==24061== at 0xc554200: ws_basestrtrou64 (strtol.c:151)
==24061== by 0xc55445A: ws_basestrtrou32 (strtol.c:248)
==24061== by 0xc554519: ws_strtrou32 (strtol.c:248)
==24061== by 0x6A913AD: bencoded_string_length (packet-bt-dht.c:107)
==24061== by 0x6A90980: dissect_bt_dht_values (packet-bt-dht.c:269)
==24061== by 0x6A902E4: dissect_bencoded_dht_entry (packet-bt-dht.c:423)
==24061== by 0x6A9009E: dissect_bencoded_dht (packet-bt-dht.c:526)
==24061== by 0x6A90259: dissect_bencoded_dht_entry (packet-bt-dht.c:416)
==24061== by 0x6A9009E: dissect_bencoded_dht (packet-bt-dht.c:526)
==24061== by 0x6A8F9D0: dissect_bt_dht (packet-bt-dht.c:598)
==24061== by 0x6A8F088: dissect_bt_dht_heur (packet-bt-dht.c:614)
==24061== by 0xd18f38A: dissector_try_heuristic (packet.c:2894)
==24061==
==24061== HEAP SUMMARY:
==24061== in use at exit: 1,386,672,711 bytes in 58,994,856 blocks
==24061== total heap usage: 202,971,252 allocs, 151,976,396 frees, 5,494,230,276 bytes allocated
==24061==
==24061== LEAK SUMMARY:
==24061== definitely lost: 0 bytes in 0 blocks
==24061== indirectly lost: 0 bytes in 0 blocks
==24061== possibly lost: 0 bytes in 0 blocks
==24061== still reachable: 1,386,556,738 bytes in 58,994,881 blocks
==24061== suppressed: 115,973 bytes in 775 blocks
==24061== Rerun with --leak-check=full to see details of leaked memory
==24061==
==24061== For lists of detected and suppressed errors, rerun with: -s
==24061== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)

fuzz-test.sh stderr:
Running as user "root" and group "root". This could be dangerous.
./tools/fuzz-test.sh: line 247: 24062 Aborted (core dumped) "$RUNNER" $COMMON_ARGS $ARGS "$TMP_DIR/$TMP_FILE"
./tools/fuzz-test.sh: line 247: 24061 CPU time limit exceeded (core dumped) "$RUNNER" $COMMON_ARGS $ARGS "$TMP_DIR/$TMP_FILE"
```

no debug trace


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  1

Relates to

 [Buildbot crash output: fuzz-2021-10-26-6706.pcap](#)
#17585

Related merge requests  5

 [BT-DHT: Fix another loop and add NULL checks.](#)

14815



 [BT-DHT: Disable heuristic for now.](#)


14816



 [BT-DHT: Fix another loop and add NULL checks.](#)


14823



 [BT-DHT: Fix another loop and add NULL checks.](#)

14848



 [BT-DHT: Fix another loop and add NULL checks.](#)

14849




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

Activity


 [A Wireshark GitterLab Utility](#) added [ci:shark](#) scoped label 1 year ago

 [A Wireshark GitterLab Utility](#) added [ci:ci](#) label 1 year ago

 [Gerald Combs](#) mentioned in merge request [14815](#) (merged) 1 year ago

 [Gerald Combs](#) made the issue visible to everyone 1 year ago

 [Gerald Combs](#) @geraldcombs · 1 year ago Owner
[@jhnthacker](#) It looks like we're getting a lot of BT-DHT false positives due to its heuristics being enabled by default in [a9f5782b](#). Is there any way to tighten them up?

 [John Thacker](#) @jhnthacker · 1 year ago Developer
I will take a look. This particular case isn't a false positive - this capture is full of what is definitely fuzzed BT-DHT, packets 16, 64, 74, 83, 235 and many more are BT-DHT.

The bencode part of the dissector just does not seem to have been tested with fuzzed input before (since it was disabled by default) and doesn't handle it well.

So I don't think it's a matter of tightening the heuristics so much as finding all the bugs. Disabling it in the 3.6 release (it's disabled in 3.4) certainly makes sense to me. I would understand if you want to disable it in the master branch as well.



John Thacker @johnthacker · 1 year ago
[4816 \(merged\)](#) created for release-3.6

Developer



A Wireshark GitLab Utility closed via merge request [4815 \(merged\)](#) 1 year ago



Gerald Combs closed via commit [79a0fa1c](#) 1 year ago



John Thacker mentioned in merge request [4821 \(merged\)](#) 1 year ago



Gerald Combs mentioned in merge request [4848 \(merged\)](#) 1 year ago



Gerald Combs mentioned in merge request [4849 \(merged\)](#) 1 year ago



Gerald Combs marked [#17685 \(closed\)](#) as a duplicate of this issue 1 year ago



Gerald Combs marked this issue as related to [#17685 \(closed\)](#) 1 year ago



Gerald Combs mentioned in commit [a138ec5d](#) 1 year ago



Gerald Combs mentioned in commit [d3c762dc](#) 1 year ago



Gerald Combs mentioned in commit [2f817bb7](#) 1 year ago

Please [register](#) or [sign in](#) to reply