

Buildbot crash output: fuzz-2020-11-05-24267.pcap

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2020-11-05-24267.pcap>

stderr:

```
Input file: /home/wireshark/menagerie/menagerie/xrite-1displaypro-argyllcms-1.9.2-spotread.pcapng

Build host information:
Linux build6 4.15.0-122-generic #124-Ubuntu SMP Thu Oct 15 13:03:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Distributor ID: Ubuntu
Description: Ubuntu 18.04.5 LTS
Release: 18.04
Codename: bionic

Buildbot information:
BUILDBOT_WORKERNAME=Fuzz-test
BUILDBOT_BUILDNUMBER=28
BUILDBOT_BUILDERNAME=Fuzz Test
BUILDBOT_URL=https://buildbot.wireshark.org/wireshark-3.4/
BUILDBOT_REPOSITORY=git@lilab.com:wireshark/wireshark.git
BUILDBOT_GOT_REVISION=a00ac1eb9c391f887b3dd56a2c508ec382790ce

Return value: 0

Dissector bug: 0

Valgrind error count: 1

Git commit
commit a00ac1eb9c391f887b3dd56a2c508ec382790ce
Author: Pau Espin Pedrol <pespin@kysomcom.de>
Date: Tue Nov 3 20:01:32 2020 +0000

    rlcmac: Handle properly LI=0 in GPRS data blocks and identify spare bits

    The previous handling of LI=0 was a confusion with the LI=0 meaning from
    EGPRS (see TS 44.060 8.8.2 Example 2) data block.

    (cherry picked from commit 9d5de22a88b9cbd01e9f16953b2e372835d3d0d6)

Command and args: ./tools/valgrind-wireshark.sh -b /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/install.plain/bin
==28634== Memcheck, a memory error detector
==28634== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==28634== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==28634== Command: /home/wireshark/builders/wireshark-3.4-fuzz/fuzztest/install.plain/bin/tshark -nr /fuzz/buildbot/fuzztest
==28634==
==28634==
==28634== HEAP SUMMARY:
==28634==     in use at exit: 317,334 bytes in 30,885 blocks
==28634==   total heap usage: 415,654 allocs, 384,769 frees, 44,723,059 bytes allocated
==28634==
==28634== LEAK SUMMARY:
==28634==    definitely lost: 276,129 bytes in 30,681 blocks
==28634==    indirectly lost: 0 bytes in 0 blocks
==28634==    possibly lost: 0 bytes in 0 blocks
==28634==    still reachable: 40,410 bytes in 173 blocks
==28634==    suppressed: 795 bytes in 31 blocks
==28634== Rerun with --leak-check=full to see details of leaked memory
==28634==
==28634== For counts of detected and suppressed errors, rerun with: -v
==28634== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
Definitely + indirectly (276129 + 0) exceeds max (102400).
```

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

Builtbot crash output: fuzz-2020-11-08-23438.pcap

#17001

Related merge requests 3

RTSP: Fixup our coherent set map.

1897

RTSP: Fixup our coherent set map.

1901

RTSP: Fixup our coherent set map.

1902

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

Activity

- [A Wireshark GitLab Utility](#) added [ci: tshark](#) scoped label 2 years ago
- [A Wireshark GitLab Utility](#) added [ci:ci](#) label 2 years ago
- [Gerald Combs](#) mentioned in merge request [1897 \(merged\)](#) 2 years ago
- [A Wireshark GitLab Utility](#) closed via merge request [1897 \(merged\)](#) 2 years ago
- [Gerald Combs](#) marked [#17001 \(closed\)](#) as a duplicate of this issue 2 years ago
- [Gerald Combs](#) marked this issue as related to [#17001 \(closed\)](#) 2 years ago
- [Gerald Combs](#) mentioned in commit [6ece1c89](#) 2 years ago
- [Gerald Combs](#) mentioned in merge request [1901 \(merged\)](#) 2 years ago
- [Gerald Combs](#) mentioned in commit [53682b53](#) 2 years ago
- [Gerald Combs](#) mentioned in merge request [1902 \(merged\)](#) 2 years ago

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