

Bug 16383 - Buildbot crash output: fuzz-2020-02-11-31730.pcap

Status: RESOLVED FIXED

Alias: None

Product: Wireshark

Component: Dissection engine (libwireshark) ([show other bugs](#))

Version: unspecified

Hardware: x86-64 Ubuntu

Importance: High Major ([vote](#))

Target Milestone: ---

Assignee: Bugzilla Administrator

URL:

Depends on:

Blocks:

Reported: 2020-02-12 00:40 UTC by Buildbot Builder

Modified: 2020-02-18 18:18 UTC ([History](#))

CC List: 0 users

See Also: ~~16360~~

Attachments

[Add an attachment](#) (proposed patch, testcase, etc.)

Note

You need to [log in](#) before you can comment on or make changes to this bug.

Buildbot Builder 2020-02-12 00:40:03 UTC [Description](#)

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2020-02-11-31730.pcap>

stderr:
Input file: /home/wireshark/menagerie/menagerie/wimax-simple-bs0-2-0.pcap

Build host information:
Linux build6 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 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=5187
BUILDBOT_BUILDDEFNAME=clang Code Analysis
BUILDBOT_URL=http://buildbot.wireshark.org/wireshark-master/
BUILDBOT_REPOSITORY=ssh://wireshark-buildbot@code.wireshark.org:29418/wireshark
BUILDBOT_GOT_REVISION=38d54660f20d53985ac3e837ce6ed3fc35839ab4

Return value: 0

Dissector bug: 0

Valgrind error count: 0

Git commit
[commit 38d54660f20d53985ac3e837ce6ed3fc35839ab4](#)
Author: Richard Sharpe <realrichardsharpe@gmail.com>
Date: Sat Feb 8 13:55:52 2020 -0500

[ieee80211-radiotap](#): Add support for radiotap TLVs.

From Johannes Berg with changes by Richard Sharpe to make it easier for people to add support for RADIOTAP Header TLVs in the future.

Change-Id: [I66d69cbe16740abce1e75cae789a2034283306b](#)
Reviewed-on: <https://code.wireshark.org/review/36057>
Reviewed-by: Richard Sharpe <realrichardsharpe@gmail.com>
Petri-Dish: Richard Sharpe <realrichardsharpe@gmail.com>
Tested-by: Petri Dish Buildbot
Reviewed-by: Johannes Berg <johannes@sipsolutions.net>
Reviewed-by: Alexis La Goutte <alexis.lagoutte@gmail.com>

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

** (process:31275): ERROR **: 00:27:47.850: Adding_ws.malformed would put more than 1000000 items in the tree -- possible infinite loop

[no debug trace]

Gerrit Code Review 2020-02-12 20:08:20 UTC [Comment 1](#)

Change 36085 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36085>

Gerrit Code Review 2020-02-13 12:17:12 UTC [Comment 2](#)

Change 36085 merged by Anders Broman:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36085>

Gerrit Code Review 2020-02-13 17:16:04 UTC [Comment 3](#)

Change 36092 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36092>

Gerrit Code Review 2020-02-13 17:16:16 UTC [Comment 4](#)

Change 36093 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36093>

Gerrit Code Review 2020-02-13 17:19:02 UTC [Comment 5](#)

Change 36094 had a related patch set uploaded by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36094>

Gerrit Code Review **2020-02-13 17:50:56 UTC**

[Comment 6](#)

Change 36092 merged by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36092>

Gerrit Code Review **2020-02-13 17:51:05 UTC**

[Comment 7](#)

Change 36093 merged by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36093>

Gerrit Code Review **2020-02-13 17:51:15 UTC**

[Comment 8](#)

Change 36094 merged by Gerald Combs:
WiMax DLMAP: Fix a large loop.

<https://code.wireshark.org/review/36094>