Bug 16258 - [oss-fuzz] Null-dereference READ in dissect_btatt

Status: RESOLVED FIXED

Alias: None

Product: Wireshark
Component: Dissection engine (libwireshark) (show other bugs)
Version: Git
Hardware: x86 macOS 10.14

Importance: Low Major (vote)
Target Milestone: ---
Assignee: Bugzilla Administrator

URL: https://bugs.chromium.org/p/oss-fuzz/...

Depends on:
Blocks:

Reported: 2019-12-06 17:02 UTC by Gerald Combs
Modified: 2020-04-09 21:28 UTC (History)
CC List: 2 users (show)

See Also: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7045

Attachments	
FUZZSHARK_TARGET=ip ./run/fuzzshark clusterfuzz-testcase-fuzzshark_ip-5767906507358208 (21.87 KB, application/octet-stream) 2019-12-06 17:02 UTC, Gerald Combs	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

Gerald Combs 2019-12-06 17:02:22 UTC **Description**

```
Created attachment 17503 [details]
FUZZSHARK_TARGET=ip ./run/fuzzshark clusterfuzz-testcase-fuzzshark_ip-
5767906507358208

Build Information:
TShark (Wireshark) 3.3.0 (v3.3.0rc0-75-g2eef68122ce2)

Copyright 1998-2019 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <https://www.gnu.org/licenses/gpl-
2.0.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with libpcap, without POSIX capabilities, with GLib 2.58.3,
with zlib 1.2.11, with SMI 0.5.0, with c-ares 1.15.0, with Lua 5.1.5, with
GnuTLS 3.6.6 and PKCS #11 support, with Gcrypt 1.8.4, with MIT Kerberos, with
MaxMind DB resolver, with nghttp2 1.36.0, with brotli, with LZ4, with Zstandard,
with Snappy, with libxml2 2.9.4.

Running on Mac OS X 10.14.6, build 18G1012 (Darwin 18.7.0), with Intel(R)
Core(TM) i9-8950HK CPU @ 2.90GHz (with SSE4.2), with 32768 MB of physical
memory, with locale en_US.UTF-8, with libpcap version 1.8.1 -- Apple version
79.250.1, with GnuTLS 3.6.6, with Gcrypt 1.8.4, with brotli 1.0.7, with zlib
1.2.11, binary plugins supported (0 loaded).

Built using clang 4.2.1 Compatible Apple LLVM 11.0.0 (clang-1100.0.33.12).
--
OSS-Fuzz found an issue with the BT ATT dissector:

$ FUZZSHARK_TARGET=ip ./run/fuzzshark /tmp/clusterfuzz-testcase-fuzzshark_ip-
5767906507358208
StandaloneFuzzTargetMain: running 1 inputs
oss-fuzzshark: disabling: snort
oss-fuzzshark: requested dissector: ip
Running: /tmp/clusterfuzz-testcase-fuzzshark_ip-5767906507358208
AddressSanitizer:DEADLYSIGNAL
=================================================================
==97002==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000069 (pc
0x00010cb59f9c bp 0x7ffee576cdc0 sp 0x7ffee576c600 T0)
==97002==The signal is caused by a READ memory access.
==97002==Hint: address points to the zero page.
    #0 0x10cb59f9b in dissect_btatt packet-btatt.c:11282
    #1 0x10e506a94 in call_dissector_work packet.c:706
    #2 0x10e5066b8 in dissector_try_uint_new packet.c:1399
    #3 0x10cbe8589 in dissect_btl2cap packet-btl2cap.c:2712
    #4 0x10e506a94 in call_dissector_work packet.c:706
    #5 0x10e506f56 in dissector_try_uint packet.c:1399
    #6 0x10d2c9942 in dissect_snap packet-llc.c:672
    #7 0x10d2c9fc9 in dissect_llc packet-llc.c:436
    #8 0x10e506a94 in call_dissector_work packet.c:706
    #9 0x10e503d55 in call_dissector_with_data packet.c:3208
    #10 0x10d14c8b0 in dissect_802_3 packet-ieee8023.c:79
    #11 0x10cee2114 in dissect_eth_common packet-eth.c:518
    #12 0x10cee0d7f in dissect_eth_withoutfcs packet-eth.c:841
    #13 0x10e506a94 in call_dissector_work packet.c:706
    #14 0x10e503d55 in call_dissector_with_data packet.c:3208
    #15 0x10d5dcd8b in dissect_bcp_bpdu packet-ppp.c
    #16 0x10e506a94 in call_dissector_work packet.c:706
    #17 0x10e506f56 in dissector_try_uint packet.c:1399
    #18 0x10d5e3e4a in dissect_ppp_common packet-ppp.c:4788
    #19 0x10d5d3e8a in dissect_ppp_raw_hdlc packet-ppp.c:6004
    #20 0x10e506a94 in call_dissector_work packet.c:706
    #21 0x10e5066b8 in dissector_try_uint_new packet.c:1399
    #22 0x10cf99c6f in dissect_gre packet-gre.c:488
    #23 0x10e506a94 in call_dissector_work packet.c:706
    #24 0x10e5066b8 in dissector_try_uint_new packet.c:1399
    #25 0x10d16bbb1 in ip_try_dissect packet-ip.c:1835
    #26 0x10d19f7cf in ipv6_dissect_next packet-ipv6.c:2545
    #27 0x10d1a0f78 in dissect_ipv6 packet-ipv6.c:2493
    #28 0x10e506a94 in call_dissector_work packet.c:706
    #29 0x10e503d55 in call_dissector_with_data packet.c:3208
    #30 0x10d16c356 in dissect_ip packet-ip.c:2321
    #31 0x10e506a94 in call_dissector_work packet.c:706
    #32 0x10e50e491 in call_all_postdissectors packet.c:3208
    #33 0x10cf40c93 in dissect_frame packet-frame.c:737
    #34 0x10e506a94 in call_dissector_work packet.c:706
    #35 0x10e503d55 in call_dissector_with_data packet.c:3208
    #36 0x10e50355e in dissect_record packet.c:580
    #37 0x10e4e8e90 in epan_dissect_run epan.c:584
    #38 0x10a495d56 in LLVMFuzzerTestOneInput fuzzshark.c:381
    #39 0x10a496c9a in main StandaloneFuzzTargetMain.c:122
    #40 0x7fff6ca193d4 in start (libdyld.dylib:x86_64+0x163d4)

==97002==Register values:
rax = 0x0000000000000000  rbx = 0x00007ffee576ccc0  rcx = 0x0000100000000000  rdx =
0x00000000000030ab
rdi = 0x0000000000000069  rsi = 0x000000000000001c  rbp = 0x00007ffee576cdc0  rsp =
0x00007ffee576c600
r8 = 0x0000100000000000  r9 = 0x000000000000000f r10 = 0x0000000000000000 r11 =
0x000000010e988a40  r12 = 0x0000000000000000 r13 = 0x0000000000000000 r14 =
0x0000000000000000 r15 = 0x0000000000000000
AddressSanitizer can not provide additional info.
```

```
SUMMARY: AddressSanitizer: SEGV packet-btatt.c:11282 in dissect_btatt
==97002==ABORTING
```

Gerrit Code Review 2019-12-06 22:32:41 UTC Comment 1

```
Change 35339 had a related patch set uploaded by Dario Lombardo:
btatt: check the opcode against the current data.

https://code.wireshark.org/review/35339
```

Gerrit Code Review 2019-12-10 08:50:00 UTC Comment 2

```
Change 35339 merged by Anders Broman:
btatt: check the opcode against the current data.

https://code.wireshark.org/review/35339
```

Gerrit Code Review 2019-12-10 09:25:30 UTC Comment 3

```
Change 35387 had a related patch set uploaded by Dario Lombardo:
btatt: check the opcode against the current data.

https://code.wireshark.org/review/35387
```

Gerrit Code Review 2019-12-10 09:25:43 UTC Comment 4

```
Change 35388 had a related patch set uploaded by Dario Lombardo:
btatt: check the opcode against the current data.

https://code.wireshark.org/review/35388
```

Gerrit Code Review 2019-12-10 10:15:23 UTC Comment 5

```
Change 35388 merged by Dario Lombardo:
btatt: check the opcode against the current data.

https://code.wireshark.org/review/35388
```

Gerrit Code Review 2019-12-10 10:15:30 UTC Comment 6

```
Change 35387 merged by Dario Lombardo:
btatt: check the opcode against the current data.

https://code.wireshark.org/review/35387
```

Format For Printing - XML - Clone This Bug - Top of page