Bug 16324 - [oss-fuzz] Global-buffer-overflow in dissect_wassp_sub_tlv

Status: RESOLVED FIXED

Alias: None

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

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

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

Depends on:
Blocks:

Reported: 2020-01-10 16:55 UTC by Gerald Combs
Modified: 2020-04-10 15:33 UTC (History)
CC List: 1 user (show)

See Also: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7044

Attachments	
FUZZSHARK_TARGET=udp ./run/fuzzshark clusterfuzz-testcase-minimized-fuzzshark_ip_proto-udp-5647238466633728 (196 bytes, application/octet-stream) 2020-01-10 16:55 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   2020-01-10 16:55:28 UTC **Description**

```
Created attachment 17559 [details]
FUZZSHARK_TARGET=udp ./run/fuzzshark clusterfuzz-testcase-minimized-
fuzzshark_ip_proto-udp-5647238466633728

Build Information:
Paste the COMPLETE build information from "Help->About Wireshark", "wireshark -v",
or "tshark -v".
--
OSS-Fuzz found an issue with the WASSP dissector:

[Environment]
ASAN_OPTIONS="alloc_dealloc_mismatch=0:allocator_may_return_null=1:allocator_release_to_os_interval_ms=500:allow_user_segv_handler=0:check_malloc_usable_size=0:detect_leaks=1:detect_odr_violation=0:detect_stack_use_after_return=1:fast_unwind_on_fatal=0:handle_abort=1:
        [Command line] python
/mnt/scratch0/clusterfuzz/src/python/bot/fuzzers/afl/launcher.py
/mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases/fuzz-1 fuzzshark_ip_proto-udp

        +----------------------------------------Release Build Stacktrace----------
------------------------------+
        Running command:
/mnt/scratch0/clusterfuzz/resources/platform/linux/minijail0 -f /tmp/tmpSXRjWN -U -
m '0 1337 1' -T static -c 0 -n -v -p -l -I -k proc,/proc,proc,1 -P
/mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases-disk/temp-171321/tmpd3bfhA -b
/mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases-disk/temp-
171321/tmptk7QL9,/tmp,1 -b /lib,/lib,0 -b /lib32,/lib32,0 -b /lib64,/lib64,0 -b
/usr/lib,/usr/lib,0 -b /usr/lib32,/usr/lib32,0 -b
/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-
afl_wireshark_9de6374568df96eba97b9288a3fce517c93d2636/revisions,/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-
builds-afl_wireshark_9de6374568df96eba97b9288a3fce517c93d2636/revisions,0 -b
/bin,/bin,0 -b /usr/bin,/usr/bin,0 -b
/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-
afl_wireshark_9de6374568df96eba97b9288a3fce517c93d2636/revisions,/out,0
/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-
afl_wireshark_9de6374568df96eba97b9288a3fce517c93d2636/revisions/fuzzshark_ip_proto-
udp /fuzz-1
        =================================================================
        ==1==ERROR: AddressSanitizer: global-buffer-overflow on address
0x000007434de8 at pc 0x000001ba4454 bp 0x7ffef7f75f10 sp 0x7ffef7f75f08
        READ of size 8 at 0x000007434de8 thread T0
        SCARINESS: 33 (8-byte-read-global-buffer-overflow-far-from-bounds)
            #0 0x1ba4453 in wassp_match_strval
/src/wireshark/epan/dissectors/packet-wassp.c:4384:32
            #1 0x1ba4453 in dissect_wassp_sub_tlv
/src/wireshark/epan/dissectors/packet-wassp.c:4779:19
            #2 0x1ba3e4c in dissect_wassp_sub_tlv
/src/wireshark/epan/dissectors/packet-wassp.c:0
            #3 0x1ba73f2 in dissect_wassp_tlv
/src/wireshark/epan/dissectors/packet-wassp.c:0
            #4 0x1ba8e8c in dissect_unfragmented_wassp
/src/wireshark/epan/dissectors/packet-wassp.c:5873:12
            #5 0x1ba8e8c in dissect_wassp /src/wireshark/epan/dissectors/packet-
wassp.c:6021:3
            #6 0x1ba7c48 in dissect_wassp_static
/src/wireshark/epan/dissectors/packet-wassp.c:7076:9
            #7 0x63bdb0 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #8 0x63bdb0 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #9 0x63c384 in dissector_try_uint_new
/src/wireshark/epan/packet.c:1399:8
            #10 0x63c384 in dissector_try_uint /src/wireshark/epan/packet.c:1423:9
            #11 0x1b01431 in decode_udp_ports
/src/wireshark/epan/dissectors/packet-udp.c:697:7
            #12 0x1b06ac8 in dissect /src/wireshark/epan/dissectors/packet-
udp.c:1234:5
            #13 0x1b03631 in dissect_udp /src/wireshark/epan/dissectors/packet-
udp.c:1240:3
            #14 0x63bdb0 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #15 0x63bdb0 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #16 0x644fd1 in call_dissector_only /src/wireshark/epan/packet.c:3208:8
            #17 0x644fd1 in call_all_postdissectors
/src/wireshark/epan/packet.c:3583:3
            #18 0xf1a832 in dissect_frame /src/wireshark/epan/dissectors/packet-
frame.c:737:5
            #19 0x63bdb0 in call_dissector_through_handle
/src/wireshark/epan/packet.c:706:9
            #20 0x63bdb0 in call_dissector_work /src/wireshark/epan/packet.c:799:9
            #21 0x63871b in call_dissector_only /src/wireshark/epan/packet.c:3208:8
            #22 0x63871b in call_dissector_with_data
/src/wireshark/epan/packet.c:3221:8
            #23 0x637eeb in dissect_record /src/wireshark/epan/packet.c:580:3
            #24 0x62bb87 in epan_dissect_run /src/wireshark/epan/epan.c:584:2
            #25 0x4ccb7e in LLVMFuzzerTestOneInput
/src/wireshark/fuzz/fuzzshark.c:381:2
            #26 0x279d3ce in ExecuteFilesOnyByOne
/src/libfuzzer/afl/afl_driver.cpp:216:5
            #27 0x279d3ce in main /src/libfuzzer/afl/afl_driver.cpp:253:12
            #28 0x7f856508282f in __libc_start_main /build/glibc-LK5gWL/glibc-
2.23/csu/libc-start.c:291
            #29 0x4203a8 in _start

        0x000007434de8 is located 8 bytes to the right of global variable
'tlvMainTable' defined in '/src/wireshark/epan/dissectors/packet-wassp.c:1369:24'
(0x742e7e0) of size 26112
        SUMMARY: AddressSanitizer: global-buffer-overflow
(/mnt/scratch0/clusterfuzz/bot/builds/clusterfuzz-builds-
afl_wireshark_9de6374568df96eba97b9288a3fce517c93d2636/revisions/fuzzshark_ip_proto-
udp+0x1ba4453)
        Shadow bytes around the buggy address:
          0x000080e7e960: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0x000080e7e970: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0x000080e7e980: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0x000080e7e990: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0x000080e7e9a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        =>0x000080e7e9b0: 00 00 00 00 00 00 00 00 00 00 00 00 f9[f9]f9 f9
          0x000080e7e9c0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
          0x000080e7e9d0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
          0x000080e7e9e0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
          0x000080e7e9f0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
          0x000080e7ea00: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
        Shadow byte legend (one shadow byte represents 8 application bytes):
          Addressable:           00
          Partially addressable: 01 02 03 04 05 06 07
          Heap left redzone:       fa
          Freed heap region:       fd
          Stack left redzone:      f1
          Stack mid redzone:       f2
          Stack right redzone:     f3
          Stack after return:      f5
          Stack use after scope:   f8
          Global redzone:          f9
          Global init order:       f6
          Poisoned by user:        f7
          Container overflow:      fc
          Array cookie:            ac
          Intra object redzone:    bb
          ASan internal:           fe
          Left alloca redzone:     ca
          Right alloca redzone:    cb
          Shadow gap:              cc
        ==1==ABORTING
```

Gerald Combs Code Review   2020-01-10 17:41:08 UTC **Comment 1**

Change 35735 had a related patch set uploaded by Gerald Combs:
WASSP: Fix a couple of off-by-one errors.

https://code.wireshark.org/review/35735

Gerrit Code Review   2020-01-12 22:49:37 UTC **Comment 2**

Change 35735 merged by Michael Mann:
WASSP: Fix a couple of off-by-one errors.

https://code.wireshark.org/review/35735

Gerrit Code Review   2020-01-13 00:45:55 UTC **Comment 3**

Change 35766 had a related patch set uploaded by Gerald Combs:
WASSP: Fix a couple of off-by-one errors.

https://code.wireshark.org/review/35766

Gerrit Code Review   2020-01-13 00:49:48 UTC **Comment 4**

Change 35766 merged by Gerald Combs:
WASSP: Fix a couple of off-by-one errors.

```
https://code.wireshark.org/review/35766
```

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