

## Fuzz job crash output: fuzz-2022-02-07-6714.pcap

Problems have been found with the following capture file:

<https://www.wireshark.org/download/automated/captures/fuzz-2022-02-07-6714.pcap>

stderr:

```
Branch: HEAD

Input file: /var/menagerie/menagerie/13895-x509-ce-distribution-points-dissection-problem.pcapng

Build host information:
Linux 5.4.0-96-generic #109-Ubuntu SMP Wed Jan 12 16:49:16 UTC 2022 x86_64
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.3 LTS
Release:        20.04
Codename:       focal

Branch: release-3.4

CI job name: ASan Menagerie Fuzz, ID: 2060427609

Return value: 0

Dissector bug: 0

Valgrind error count: 0

Latest (but not necessarily the problem) commit:
e9c3dfe05 [Automatic update for 2022-02-06]
Command and args: /builds/wireshark/wireshark/_install/bin/tshark -2 -nVxr
Running as user "root" and group "root". This could be dangerous.
=====
==87972==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000886420 at pc 0x5604c9392069
READ of size 28 at 0x606000886420 thread T0
#0 0x5604c9392068 in strlen (/builds/wireshark/wireshark/_install/bin/tshark+0x6e068)
#1 0x7f9e573a6147 in g_strdup (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x72147)
#2 0x7f9e63f2bc6b in find_string_dtbl_entry /builds/wireshark/wireshark/build/./epan/packet.c:1
#3 0x7f9e63f2c041 in dissector_try_string_new /builds/wireshark/wireshark/build/./epan/packet.c
#4 0x7f9e63f2c206 in dissector_try_string /builds/wireshark/wireshark/build/./epan/packet.c:173
#5 0x7f9e610e26d in call_ber_oid_callback /builds/wireshark/wireshark/build/./epan/dissectors/
#6 0x7f9e631995f1 in dissect_cms_T_parameters /builds/wireshark/wireshark/build/./asn1/cms/cms.c
#7 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/p
#8 0x7f9e63199477 in dissect_cms_SMIMECapabilities /builds/wireshark/wireshark/build/./asn1/cms/cm
#9 0x7f9e61020437 in dissect_ber_sq_of /builds/wireshark/wireshark/build/./epan/dissectors/pack
#10 0x7f9e610206f2 in dissect_ber_sequence_of /builds/wireshark/wireshark/build/./epan/dissecto
#11 0x7f9e63199407 in dissect_cms_SMIMECapabilities /builds/wireshark/wireshark/build/./asn1/cms
#12 0x7f9e63194397 in dissect_SMIMECapabilities_PDU /builds/wireshark/wireshark/build/./asn1/cms
#13 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#14 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#15 0x7f9e63f2c136 in dissector_try_string_new /builds/wireshark/wireshark/build/./epan/packet.
#16 0x7f9e63f2c206 in dissector_try_string /builds/wireshark/wireshark/build/./epan/packet.c:17
#17 0x7f9e610e26d in call_ber_oid_callback /builds/wireshark/wireshark/build/./epan/dissectors
#18 0x7f9e63ba9279 in dissect_x509af_T_extnValue /builds/wireshark/wireshark/build/./asn1/x509af
#19 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/
#20 0x7f9e63ba6447 in dissect_x509af_Extension /builds/wireshark/wireshark/build/./asn1/x509af/x
#21 0x7f9e61020437 in dissect_ber_sq_of /builds/wireshark/wireshark/build/./epan/dissectors/pac
#22 0x7f9e610206f2 in dissect_ber_sequence_of /builds/wireshark/wireshark/build/./epan/dissecto
#23 0x7f9e63ba64b7 in dissect_x509af_Extensions /builds/wireshark/wireshark/build/./asn1/x509af/
#24 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/
#25 0x7f9e63ba9367 in dissect_x509af_T_signedCertificate /builds/wireshark/wireshark/build/./asn
#26 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/
#27 0x7f9e63ba6527 in dissect_x509af_Certificate /builds/wireshark/wireshark/build/./asn1/x509af
#28 0x7f9e6293c5e9 in ssl_dissect_hnd_cert /builds/wireshark/wireshark/build/./epan/dissectors/
#29 0x7f9e629656ca in dissect_tls_handshake_full /builds/wireshark/wireshark/build/./epan/disse
#30 0x7f9e629632fa in dissect_tls_handshake /builds/wireshark/wireshark/build/./epan/dissectors
#31 0x7f9e6295ed72 in dissect_ssl3_record /builds/wireshark/wireshark/build/./epan/dissectors/p
```

```

#32 0x7f9e6295aa21 in dissect_ssl /builds/wireshark/wireshark/build/./epan/dissectors/packet-tl
#33 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#34 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#35 0x7f9e63f32a20 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:323
#36 0x7f9e63f27024 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.
#37 0x7f9e63f32a61 in call_dissector /builds/wireshark/wireshark/build/./epan/packet.c:3263:9
#38 0x7f9e61642dd2 in dissect_eap /builds/wireshark/wireshark/build/./epan/dissectors/packet-ea
#39 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#40 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#41 0x7f9e63f2a919 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:
#42 0x7f9e61649839 in dissect_eapol /builds/wireshark/wireshark/build/./epan/dissectors/packet-
#43 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#44 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#45 0x7f9e63f2a919 in dissector_try_uint_new /builds/wireshark/wireshark/build/./epan/packet.c:
#46 0x7f9e63f2b3eb in dissector_try_uint /builds/wireshark/wireshark/build/./epan/packet.c:1437
#47 0x7f9e61d70341 in dissect_snap /builds/wireshark/wireshark/build/./epan/dissectors/packet-l
#48 0x7f9e61d71134 in dissect_llc /builds/wireshark/wireshark/build/./epan/dissectors/packet-ll
#49 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#50 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#51 0x7f9e63f32a20 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:323
#52 0x7f9e63f27024 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.
#53 0x7f9e63f32a61 in call_dissector /builds/wireshark/wireshark/build/./epan/packet.c:3263:9
#54 0x7f9e61aa467a in dissect_ieee80211_common /builds/wireshark/wireshark/build/./epan/dissect
#55 0x7f9e61a74706 in dissect_ieee80211 /builds/wireshark/wireshark/build/./epan/dissectors/pac
#56 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#57 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#58 0x7f9e63f32a20 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:323
#59 0x7f9e63f27024 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.
#60 0x7f9e61a4e021 in dissect_wlan_radio /builds/wireshark/wireshark/build/./epan/dissectors/pa
#61 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#62 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#63 0x7f9e63f32a20 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:323
#64 0x7f9e63f27024 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.
#65 0x7f9e61a60959 in dissect_radiotap /builds/wireshark/wireshark/build/./epan/dissectors/pack
#66 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#67 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#68 0x7f9e63f32a20 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:323
#69 0x7f9e6175f8b6 in dissect_frame /builds/wireshark/wireshark/build/./epan/dissectors/packet-
#70 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#71 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#72 0x7f9e63f32a20 in call_dissector_only /builds/wireshark/wireshark/build/./epan/packet.c:323
#73 0x7f9e63f27024 in call_dissector_with_data /builds/wireshark/wireshark/build/./epan/packet.
#74 0x7f9e63f2680f in dissect_record /builds/wireshark/wireshark/build/./epan/packet.c:594:3
#75 0x7f9e63ef5f88 in epan_dissect_run_with_taps /builds/wireshark/wireshark/build/./epan/epan.
#76 0x5604c945e357 in process_packet_second_pass /builds/wireshark/wireshark/build/./tshark.c:3
#77 0x5604c945c88e in process_cap_file_second_pass /builds/wireshark/wireshark/build/./tshark.c
#78 0x5604c94569b6 in process_cap_file /builds/wireshark/wireshark/build/./tshark.c:3650:28
#79 0x5604c94504c8 in main /builds/wireshark/wireshark/build/./tshark.c:2102:16
#80 0x7f9e5711e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#81 0x5604c937f43d in _start (/builds/wireshark/wireshark/_install/bin/tshark+0x5b43d)

```

0x60600088643b is located 0 bytes to the right of 59-byte region [0x606000886400,0x60600088643b)  
freed by thread T0 here:

```

#0 0x5604c93f78fd in free (/builds/wireshark/wireshark/_install/bin/tshark+0xd38fd)
#1 0x7f9e63e00f03 in wmem_free /builds/wireshark/wireshark/build/./epan/wmem/wmem_core.c:65:9
#2 0x7f9e63e0b01b in wmem_strict_free /builds/wireshark/wireshark/build/./epan/wmem/wmem_alloc
#3 0x7f9e63e0b0c4 in wmem_strict_free_all /builds/wireshark/wireshark/build/./epan/wmem/wmem_al
#4 0x7f9e63e01279 in wmem_free_all_real /builds/wireshark/wireshark/build/./epan/wmem/wmem_core
#5 0x7f9e63e011d6 in wmem_free_all /builds/wireshark/wireshark/build/./epan/wmem/wmem_core.c:11
#6 0x7f9e63e10a1a in wmem_leave_packet_scope /builds/wireshark/wireshark/build/./epan/wmem/wmem
#7 0x7f9e63ef5f2d in epan_dissect_run /builds/wireshark/wireshark/build/./epan/epan.c:588:2
#8 0x5604c945db37 in process_packet_first_pass /builds/wireshark/wireshark/build/./tshark.c:302
#9 0x5604c945bf2f in process_cap_file_first_pass /builds/wireshark/wireshark/build/./tshark.c:3
#10 0x5604c945696c in process_cap_file /builds/wireshark/wireshark/build/./tshark.c:3631:25
#11 0x5604c94504c8 in main /builds/wireshark/wireshark/build/./tshark.c:2102:16
#12 0x7f9e5711e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

```

previously allocated by thread T0 here:

```

#0 0x5604c93f7b7d in malloc (/builds/wireshark/wireshark/_install/bin/tshark+0xd3b7d)
#1 0x7f9e5738be98 in g_malloc (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x57e98)
#2 0x7f9e63e0a8ab in wmem_strict_alloc /builds/wireshark/wireshark/build/./epan/wmem/wmem_alloc
#3 0x7f9e63e0ac94 in wmem_strict_realloc /builds/wireshark/wireshark/build/./epan/wmem/wmem_all

```

```
#4 0x7f9e63e011b0 in wmem_realloc /builds/wireshark/wireshark/build/./epan/wmem/wmem_core.c:96:
#5 0x7f9e63e1327c in wmem_strbuf_finalize /builds/wireshark/wireshark/build/./epan/wmem/wmem_st
#6 0x7f9e63f1d4dc in rel_oid_subid2string /builds/wireshark/wireshark/build/./epan/oids.c:898:9
#7 0x7f9e63f18a07 in oid_subid2string /builds/wireshark/wireshark/build/./epan/oids.c:875:9
#8 0x7f9e63f1f5f4 in oid_encoded2string /builds/wireshark/wireshark/build/./epan/oids.c:1164:9
#9 0x7f9e6101dd26 in dissect_ber_any_oid_str /builds/wireshark/wireshark/build/./epan/dissector
#10 0x7f9e6101dec2 in dissect_ber_object_identifier_str /builds/wireshark/wireshark/build/./epa
#11 0x7f9e631994df in dissect_cms_T_capability /builds/wireshark/wireshark/build/./asn1/cms/cms.
#12 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/
#13 0x7f9e63199477 in dissect_cms_SMIMECapability /builds/wireshark/wireshark/build/./asn1/cms/c
#14 0x7f9e61020437 in dissect_ber_sq_of /builds/wireshark/wireshark/build/./epan/dissectors/pac
#15 0x7f9e610206f2 in dissect_ber_sequence_of /builds/wireshark/wireshark/build/./epan/dissecto
#16 0x7f9e63199407 in dissect_cms_SMIMECapabilities /builds/wireshark/wireshark/build/./asn1/cms
#17 0x7f9e63194397 in dissect_SMIMECapabilities_PDU /builds/wireshark/wireshark/build/./asn1/cms
#18 0x7f9e63f361d1 in call_dissector_through_handle /builds/wireshark/wireshark/build/./epan/pa
#19 0x7f9e63f2b000 in call_dissector_work /builds/wireshark/wireshark/build/./epan/packet.c:813
#20 0x7f9e63f2c136 in dissector_try_string_new /builds/wireshark/wireshark/build/./epan/packet.
#21 0x7f9e63f2c206 in dissector_try_string /builds/wireshark/wireshark/build/./epan/packet.c:17
#22 0x7f9e6100e26d in call_ber_oid_callback /builds/wireshark/wireshark/build/./epan/dissectors
#23 0x7f9e63ba9279 in dissect_x509af_T_extnValue /builds/wireshark/wireshark/build/./asn1/x509af
#24 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/
#25 0x7f9e63ba6447 in dissect_x509af_Extension /builds/wireshark/wireshark/build/./asn1/x509af/x
#26 0x7f9e61020437 in dissect_ber_sq_of /builds/wireshark/wireshark/build/./epan/dissectors/pac
#27 0x7f9e610206f2 in dissect_ber_sequence_of /builds/wireshark/wireshark/build/./epan/dissecto
#28 0x7f9e63ba64b7 in dissect_x509af_Extensions /builds/wireshark/wireshark/build/./asn1/x509af/
#29 0x7f9e61017bed in dissect_ber_sequence /builds/wireshark/wireshark/build/./epan/dissectors/
```

SUMMARY: AddressSanitizer: heap-use-after-free (/builds/wireshark/wireshark/\_install/bin/tshark+0x6e  
Shadow bytes around the buggy address:

```
0x0c0c80108c30: fd fd fd fd fa fa fa fd fd fd fd fd fd fd fa
0x0c0c80108c40: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa
0x0c0c80108c50: fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c80108c60: fd fd fd fa fa fa fa fd fd fd fd fd fd fa
0x0c0c80108c70: fa fa fa fa fd fd fd fd fd fd fa fa fa fa
=>0x0c0c80108c80: fd fd fd fd[fd]fd fd fd fa fa fa fd fd fd fd
0x0c0c80108c90: fd fd fd fa fa fa fa 00 00 00 00 00 00 00
0x0c0c80108ca0: fa fa fa fa fd fd fd fd fd fd fa fa fa fa
0x0c0c80108cb0: fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c80108cc0: fd fd fd fd fa fa fa 00 00 00 00 00 00 00
0x0c0c80108cd0: fa fa fa fa fd fd fd fd fd fd fa fa fa fa
```

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

==87972==ABORTING

fuzz-test.sh stderr:


Running as user "root" and group "root". This could be dangerous.

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  0

Link issues together to show that they're related or that one is blocking others. [Learn more.](#)

Related merge requests  2

 [CMS: get rid of globals](#)

!6160



 [CMS: get rid of globals](#)


!6161



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

## Activity

 [A Wireshark GitLab Utility](#) added `cli` `tshark` scoped label 9 months ago

 [A Wireshark GitLab Utility](#) added `crash` label 9 months ago



[John Thacker](#) @johnthacker · 9 months ago

Developer

This is on `release-3.4`, and the issue should be fixed on `master` by [c14d731e](#) which got rid of the global `object_identifier_id` that is of issue here. (There's a SEQUENCE OF SMIMECapabilities and the oid is wrong in the first one. First pass, it doesn't exist, second pass, the global is still pointing to a packet scoped now freed string generated from a later member of the sequence in the first pass.)

So it's a question of whether it's worth backporting the fix to 3.4 (and 3.6)




[Gerald Combs](#) @geraldcombs · 9 months ago

Owner


I think it's worth backporting (in progress in [!6160 \(merged\)](#) and [!6161 \(merged\)](#)), but I'm not sure if this requires a CVE.

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

 [Gerald Combs](#) made the issue visible to everyone 9 months ago

 [John Thacker](#) mentioned in commit [b0f679bb](#) 9 months ago

 [John Thacker](#) mentioned in commit [9369af77](#) 9 months ago

 [Gerald Combs](#) closed 9 months ago



[Gerald Combs](#) @geraldcombs · 9 months ago

Owner

This has been assigned CVE-2022-0581.

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