

Wireshark stability - multiple dissector bugs - runtime errors

Summary

This is my naive attempt to fix (hopefully) all of Wireshark dissector runtime errors. In the last few weeks ran fuzzers and wrote some tools to find and disclose security and stability bugs with the sole goal of making Wireshark as stable as possible. I've gathered a decent list of naughty dissectors that are passing NULL pointers to functions when they shouldn't. Obviously this could cause undefined behaviors in runtime and sometimes even crash Wireshark/tshark - runtime error: null pointer passed as argument .

I decided to concentrate everything into a single issue so I won't spam with many "NULL pointer is passed" issues.

To reproduce these issues, one would need to compile tshark with address sanitizers (and specifically UBS - UndefinedBehaviorSanitizer). There are 5 main categories of runtime errors:

1. NULL pointer passed to `bytes_to_str_punct_maxlen()`
2. NULL pointer passed as argument to `epan/tvbuff.c:932:17`
3. NULL pointer passed as argument to `wsutil/wmem/wmem_array.c:119:63`
4. Store to misaligned address
5. X is outside the range of representable values of type `unsigned int`

[Fixed?] Dissector

- ☒ ZigBee-ZCL
- ☒ ACF-LIN
- ☒ ACF-CAN
- ☒ ANSI C12.22
- ☒ SMB2 (SMB3)
- ☒ CIP
- ☒ DTLS
- ☒ LTP
- ☒ SSLv3
- ☒ CSN1 (X2AP)
- ☒ DNS
- ☒ SNMP
- ☒ ENIP
- ☒ Bundle
- ☒ NBAP
- ☒ TCP
- ☒ CoAP
- ☒ IPDC
- ☒ CL-PRES
- ☒ 802.11
- ☒ NFS
- ☒ DCERPC
- ☒ RPC
- ☒ BPv7
- ☒ 5co-legacy
- ☒ 6LoWPAN
- ☒ JXTA

Samples

ZigBee-ZCL (zbee_zcl)

```
** (tshark:66662) 17:07:59.843905 [(none) CRITICAL] wsutil/to_str.c:229 -- bytes_to_str_punct_maxle
0.000000      1 00:00:a0:45:df:06:a6:26 -> 0x0101      ZigBee  ZCL: Write Attributes No Response, S
```

- pcap: [zbee_zero_length_passed_to_bytes_to_str_punct_max.pcapng](#)

ACF-LIN

```
** (tshark:66684) 17:08:05.983981 [(none) CRITICAL] wsutil/to_str.c:229 -- bytes_to_str_punct_maxle
0.000000      1 00:00:06:66:29:21 → 70:b3:d5:8e:f6:de ACF-LIN ACF-LIN(31): 0xfb fb fb 116
```

- pcap: [tshark:66684.acf-lin_zero_length_passed_to_bytes_to_str_punct_max.pcapng](#)

ACF-CAN

```
** (tshark:66710) 17:08:15.849287 [(none) CRITICAL] wsutil/to_str.c:229 -- bytes_to_str_punct_maxle
0.000000      1 00:00:00:66:29:21 → 70:b3:d5:8e:f6:de ACF-CAN ACF-CAN(4): 0x04040404 7c 50 00 00
```

- pcap: [tshark:66710.acf-can_zero_length_passed_to_bytes_to_str_punct_max.pcapng](#)

ANSI C12.22

```
tshark_errors/error/e607ffef414486cb75738d15e41a7fbea057137a.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 ANSI C12.22 169 1153 → 36659 [PSH, CWR, Reserved]
```

- pcap: [tshark_errors/error/e607ffef414486cb75738d15e41a7fbea057137a.pcap](#)

SMB2 (SMB3)

```
tshark_errors/error/f85d55d45096d2b94e9794ea7342935770fc70aa.pcap
../wsutil/wmem/wmem_array.c:119:63: runtime error: null pointer passed as argument 2, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../wsutil/wmem/wmem_array.c:119:63 in
../epan/tvbuff_lznt1.c:135:10: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff_lznt1.c:135:10 in
1 0.000000 170.170.170.170 → 170.170.170.170 SMB2 112 Decom. SMB3[BoundErrorUnreassembled Packet]
```

```
tshark_errors/error/762ec73eaa1361726383f30fa3e1d6c787c5d9fe.pcap
../wsutil/wmem/wmem_array.c:119:63: runtime error: null pointer passed as argument 2, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../wsutil/wmem/wmem_array.c:119:63 in
1 0.000000 170.170.170.170 → 170.170.170.170 SMB2 120 Comp. SMB3 (unknown)
```

- pcap: [tshark_errors/error/f85d55d45096d2b94e9794ea7342935770fc70aa.pcap](#) [tshark_errors/error/762ec73eaa1361726383f30fa3e1d6c787c5d9fe.pcap](#)

CIP

```
tshark_errors/error/2a616f06df5882de9dbf1925fa6e3843e14dc078.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 CIP 109 Multiple Service Packet: Start, [BoundErrorUnreassembled Packet]
```

```
tshark_errors/error/a513e0347ba7c4f33abc310247c0644e03fc22ae.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 CIP 108 Service (0x00)
```

- pcap: [2a616f06df5882de9dbf1925fa6e3843e14dc078.pcap](#)
[a513e0347ba7c4f33abc310247c0644e03fc22ae.pcap](#)

DTLS

```
tshark_errors/error/14041d11455b0a6fdc9a940ff356982be32142dd.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 DTLS 1.0 (OpenSSL pre 0.9.8f) 112 Certificate Req
```

- pcap:
-
- [14041d11455b0a6fdc9a940ff356982be32142dd.pcap](#)

LTP

```
tshark_errors/error/1901d52c701302cf5de33c95f652b64e532dade8.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 LTP Segment 101 Protocol Error
```

- pcap:
-
- [1901d52c701302cf5de33c95f652b64e532dade8.pcap](#)

SSLv3

```
tshark_errors/error/94be5d690a7301ade3e70769a1f1dbc9a3e3df7.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 SSLv3 124 New Session Ticket, New Session Ticket,
```

```
tshark_errors/error/30a018ee7c96129f081ca38dda267cd83139095b.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 SSLv3 124 End of Early Data, New Session Ticket.
```

- pcap: [94be75d690a7301ade3e70769a1f1dbc9a3e3df7.pcap](#)
[30a018ee7c96129f081ca38dda267cd83139095b.pcap](#)

CSN1 (X2AP)

[illegible]

SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/dissectors/packet-csn1.c:773:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 X2AP 117 ENDCConfigurationTransfer, MobilityFromE

[illegible]

SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/dissectors/packet-csn1.c:773:17 in
1 0.000000 170.170.170.170 → 170.170.170.170 X2AP 116 GNBStatusIndication, MobilityFromEUTRACo

- pcap: [5da74e09f3d5a3a0af8d8c8a6142bf644217bcc0.pcap](#)
dd7fe5d01f155faebb8021e22a2fa27c9d2b9825.pcap

DNS

```
tshark_errors/error/746d5475691e3bd7b74e7a78ae3cd9491d9f724d.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 DNS 151 Unknown operation (9) 0x0000 HTTPS[BoundErrorUnre]

tshark_errors/error/1d3bb7805e95fba0ae43bc87ec0963acc13a32f4.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 DNS 154 Standard query 0x0267 SVCB[BoundErrorUnre]
```

- pcap: [tshark_errors/error/746d5475691e3bd7b74e7a78ae3cd9491d9f724d.pcap](#)
- [tshark_errors/error/1d3bb7805e95fba0ae43bc87ec0963acc13a32f4.pcap](#)

SNMP

```
tshark_errors/error/42458338bed52e817ef07d6caa391106bf9a3a3e.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 SNMP 126 get-response itu-t
```

- pcap: [tshark_errors/error/42458338bed52e817ef07d6caa391106bf9a3a3e.pcap](#)

ENIP

```
tshark_errors/error/64112d632148396fe46936637ca6e019c40bb53d.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 ENIP 119 Get Attribute List | Unknown Command (0x00000000)
```

- pcap: [tshark_errors/error/64112d632148396fe46936637ca6e019c40bb53d.pcap](#)

Bundle

```
tshark_errors/error/88b8ef634bfa18e1ec595a9b0d6382637ce8f827.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 Bundle 106 Protocol Error
```

- pcap: [tshark_errors/error/88b8ef634bfa18e1ec595a9b0d6382637ce8f827.pcap](#)

NBAP

```
tshark_errors/error/f33b37100c1014ebde8859eb17c23021c47ed010.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 NBAP 123 id-cellReconfiguration (MasterInformationElement)
```

- pcap: [tshark_errors/error/f33b37100c1014ebde8859eb17c23021c47ed010.pcap](#)

TCP

```
tshark_errors/error/22247efd63b724b44633847393617375d026d315.pcap
../epan/tvbuff.c:2232:35: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:92:34: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:2232:35 in
1  0.000000 196.0.0.0 → 0.0.160.158 TCP 129 54051 → 30028 [SYN, PSH, ACK, CWR, Reserved] Seq=1960000000, Win=0, Len=0

tshark_errors/error/ea86b73f7579aa746d04ba6d186c52f6497d8f4e.pcap
../epan/tvbuff.c:2232:35: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:92:34: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:2232:35 in
1  0.000000 0.0.0.0 → 160.158.211.35 TCP 127 30028 → 28928 [SYN, PSH, ACK, CWR, Reserved] Seq=0, Win=0, Len=0
```

- pcap: [tshark_errors/error/22247efd63b724b44633847393617375d026d315.pcap](#)
- [tshark_errors/error/ea86b73f7579aa746d04ba6d186c52f6497d8f4e.pcap](#)

CoAP

```
tshark_errors/error/feada1a8b3048fd4b263cbfd2c8f4932f77b007e.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 CoAP 143 RST, MID:32667, Unknown 255[BoundErrorUn
```

- pcap: [tshark_errors/error/feada1a8b3048fd4b263cbfd2c8f4932f77b007e.pcap](#)

IPDC

```
tshark_errors/error/8583c6e8b477b0b8a15e31ac207a02d8abf50200.pcap
../epan/dissectors/packet-ipdc.c:828:25: runtime error: 2.69599e+67 is outside the range of representable values
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/dissectors/packet-ipdc.c:828:25 in
1  0.000000 170.170.170.170 → 170.170.170.170 IPDC 126 14001 → 6668 [PSH, URG, NS, Reserved] Seq=1700000000, Win=0, Len=0
```

- pcap: [tshark_errors/error/8583c6e8b477b0b8a15e31ac207a02d8abf50200.pcap](#)

CL-PRES

```
tshark_errors/error/6d96ffe15d77326b3877e1837ba633d3bc2df741.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 CL-PRES 122 [Malformed Packet]
```

- pcap: [tshark_errors/error/6d96ffe15d77326b3877e1837ba633d3bc2df741.pcap](#)

802.11

```
tshark_errors/error/6d9b3270b75a036f6ccff68aed5a863add4084dc.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 802.11 167 PV1 Management[Malformed Packet]
```

- pcap: [tshark_errors/error/6d9b3270b75a036f6ccff68aed5a863add4084dc.pcap](#)

NFS

```
tshark_errors/error/e2d684637c2c6810639d33d11b1fd95adf94b169.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 NFS CB 119 FragmentFragmentFragment ; V384460390
```

- pcap: [tshark_errors/error/e2d684637c2c6810639d33d11b1fd95adf94b169.pcap](#)

DCERPC

```
tshark_errors/error/7c04dfdd49cef00fa85cebf2a7af47181a12f9ad.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 DCERPC 134 RPC-over-HTTP RTS: call_id: 12763842,
```

- pcap: [tshark_errors/error/7c04dfdd49cef00fa85cebf2a7af47181a12f9ad.pcap](#)

RPC

```
tshark_errors/error/d6ca8adc49c920a3e628c909e144b717112eb236.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 RPC 116 FragmentFragmentFragmentFragment
```

- pcap: [tshark_errors/error/d6ca8adc49c920a3e628c909e144b717112eb236.pcap](#)

BPv7

```
tshark_errors/error/34c6678ceeeb0676f126bd8fd3c4a60a53cbbf2b.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 BPv7 80 [Malformed Packet]
```

- pcap: [tshark_errors/error/34c6678ceeeb0676f126bd8fd3c4a60a53cbbf2b.pcap](#)

5co-legacy

```
tshark_errors/error/bd87afea90f7f96919d2af8895c3fb2ddb6c9d54.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 170.170.170.170 → 170.170.170.170 5co-legacy 126 I2C Read and write with ack ID=179
```

- pcap: [tshark_errors/error/bd87afea90f7f96919d2af8895c3fb2ddb6c9d54.pcap](#)

6LoWPAN

```
tshark_errors/error/695ec0c3565e61008b761ccb37bb9351efb2c1b2.pcap
../epan/tvbuff.c:932:17: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:44:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:932:17 in
1  0.000000 0x8888 → 6LoWPAN 101 Data, Src: 0x8888[BoundErrorUnreassembled P
```

- pcap: [695ec0c3565e61008b761ccb37bb9351efb2c1b2.pcap](#)

JXTA

```
tshark_errors/error/daa5b5267078cc99209152a253546e0665989768.pcap
../epan/tvbuff.c:2232:35: runtime error: null pointer passed as argument 1, which is declared to nev
/usr/include/string.h:92:34: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../epan/tvbuff.c:2232:35 in
1 0.000000 136.136.136.136 → 136.131.18.2 JXTA 129 Welcome
```

- pcap: [daa5b5267078cc99209152a253546e0665989768.pcap](#)

Build information

TShark (Wireshark) 3.7.0 (v3.7.0rc0-844-g14a1dfbe1083)

Edited 9 months ago by [Sharon Brizinov](#)

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 19	
tvbuff: add robustness to memory copy related functions	
!5899	
IPDC: implement proper length checks	
!5900	
Fix NULL arg calls to bytes to str punct maxlen.	
!5922	
tvbuff: add robustness to tvb search related functions	
!5928	
TVB: Don't uncompress zero sized buffers	
!5947	
tvbuff: add robustness to memory copy related functions	
!6011	
tvbuff: add robustness to memory copy related functions	
!6012	
IPDC: implement proper length checks	
!6013	
IPDC: implement proper length checks	
!6014	
tvbuff: assert the called len is > 0.	
!6015	
tvbuff: assert the called len is > 0.	
!6016	
tvbuff: add robustness to tvb search related functions	

!6017		
 tvbuff: add robustness to tvb search related functions		
!6018		
 TVB: Don't uncompress zero sized buffers		
!6019		
 TVB: Don't uncompress zero sized buffers		
!6020		
 CSN.1: Fix some alignment issues.		
!6055		
 CSN.1: Fix some alignment issues.		
!6127		
 CSN.1: Fix some alignment issues.		
!6128		
 CSN.1: Fix compiler warning showing wrong copy.		
!6265		

Activity

	Sharon Brizinov changed the description 10 months ago ·	
	Sharon Brizinov changed the description 10 months ago ·	
	Sharon Brizinov @sean007 · 10 months ago <div> Author Contributor </div> @geraldcombs I accidentally made this public and can't hide this. Can you please make it hidden?	
	Sharon Brizinov marked the checklist item ANSI C12.22 as completed 10 months ago	
	Sharon Brizinov marked the checklist item ANSI C12.22 as incomplete 10 months ago	
	Sharon Brizinov changed the description 10 months ago ·	
	Pascal Quantin made the issue confidential 10 months ago	
	Pascal Quantin @pquantin · 10 months ago <div>Developer</div> The X2AP bug is actually a CSN1 one.	
	Sharon Brizinov changed the description 10 months ago ·	
	Jaap Keuter mentioned in merge request !5899 (merged) 10 months ago	
	Jaap Keuter mentioned in merge request !5900 (merged) 10 months ago	
	Dario Lombardo @crondaemon · 10 months ago <div>Developer</div> Hi @sean007 , the fix from @JaapKeuter fixed a bunch of dissector errors. Can you please mark the fixed ones for an easier follow up on the outstanding?	
	Dario Lombardo @crondaemon · 10 months ago <div>Developer</div> <h2>bytes_to_str_punct_maxlen</h2> <p>This case is already handled by wireshark. Indeed no crash, no messages such as "dissector bug" appear, nothing out-of-ordinary. However when a packet-driven null string is passed to this function, a warning appears in console. It sounds a bit overkill to me, since they are packet-driven data. My suggestion is to lower this log level to debug, to shut it up unless desired.</p>	



[João Valverde](#) @jvalverde · 10 months ago

Developer

Something out-of-the-ordinary does happen, the function returns a meaningless placeholder value when it receives a null string. This is a bug. It is an error to pass NULL to this function.



[Dario Lombardo](#) @crondaemon · 10 months ago

Developer

Which fix would you suggest?



[João Valverde](#) @jvalverde · 10 months ago

Developer

It is a failed assertion so naturally the fix is to not pass an invalid input to this function. I think it's going to required a case-by-case analysis of the calling logic.



[Dario Lombardo](#) @crondaemon · 10 months ago

Developer

Fix proposal in [!5922 \(merged\)](#).

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



[Guy Harris](#) @guyharris · 10 months ago

Maintainer

The X2AP bug is actually a CSN1 one.

And the bug is that it's storing the decoded data into what amounts to a packed structure by doing assignments with unaligned pointers rather than doing `memcpy()`.

A SPARC - or ARM? - machine will haunt you forever in your dreams if you do that. (At least with SPARC you get an alignment fault; ARM may just give you unexpected behavior.)



[Jaap Keuter](#) @JaapKeuter · 10 months ago

Developer

Can confirm ARM may give you a data abort over unaligned access, either through CP15 setting or page table attributes. Working on such a gremlin right now.

Edited by [Jaap Keuter](#) 10 months ago

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



[Sharon Brizinov](#) marked the checklist item **IPDC** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **ANSI C12.22** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **CIP** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **DTLS** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **LTP** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **SSLv3** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **DNS** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **SNMP** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **ENIP** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **Bundle** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **NBAP** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **CoAP** as completed [10 months ago](#)

- ✓ [Sharon Brizinov](#) marked the checklist item **CL-PRES** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **802.11** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **NFS** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **6LoWPAN** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **5co-legacy** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **BPv7** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **RPC** as completed [10 months ago](#)
- ✓ [Sharon Brizinov](#) marked the checklist item **DCERPC** as completed [10 months ago](#)
- ✎ [Sharon Brizinov](#) changed the description [10 months ago](#) ·



[Sharon Brizinov](#) @sean007 · 10 months ago

Author

Contributor

I prepared a merged pcap with all the samples above so it will be easier to test what is fixed [fix merged tshark runtime errors.pcapng](#)
can you please mark this issue as crash ?



[Alexis La Goutte](#) added [crash](#) label [10 months ago](#)



[Dario Lombardo](#) mentioned in merge request [!5922 \(merged\)](#) [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **ZigBee-ZCL** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **ACF-LIN** as completed [10 months ago](#)



[Sharon Brizinov](#) marked the checklist item **ACF-CAN** as completed [10 months ago](#)



[Jaap Keuter](#) mentioned in merge request [!5928 \(merged\)](#) [10 months ago](#)



[Sharon Brizinov](#) @sean007 · 10 months ago

Author

Contributor

This discussion made me think about all the failed assertions in the dissectors which produce errors in Wireshark

For example - I was able to trigger a warning/error in the TLS dissector due to failed assertion (I'm not sure why such an assertion was written instead of stating malformed packet) -

```
** (wireshark:72362) 23:27:42.521848 [Epan WARNING] -- Dissector bug, protocol TLS, in p
```

[fix tls warning failed assertion.pcap](#)

Do we want to fix these? if so, I can hunt all of these cases and generate a pcap reproducer for each case just like I did here.

Edited by [Sharon Brizinov](#) 10 months ago



[João Valverde](#) @jvalverde · 10 months ago

Developer

Yes, of course. Any failed assertion is a bug that needs to be fixed.



[Guy Harris](#) @guyharris · 10 months ago

Maintainer

Anything in the dissection that says "Dissector Bug" is, as it says on the tin, a dissector bug. (Well, with the obvious exception of, for example, the HTML reply from a GET request when the page being fetched has the title "Dissector Bug". :-))



Sharon Brizinov @sean007 · 10 months ago

Author

Contributor

No problem. I'm on it. The next stable version of Wireshark (v3.6.2?) will be the most stable and secure version ever existed 😊

BTW - I have many more ideas for making Wireshark more secure and stable. Is there a Slack/Telegram/Discord/Whatever channel we could discuss this internally?

Edited by [Sharon Brizinov](#) 10 months ago



Dario Lombardo @crondaemon · 10 months ago

Developer

The dev mailing list is the proper place: wireshark-dev@wireshark.org.



Alexis La Goutte @alagoutte · 10 months ago

Developer

There is also Wireshark developer den (the next is planned Tuesday, February 1st, more info on [wireshark-dev](#))



Alexis La Goutte @alagoutte · 10 months ago

Developer

What fuzzer do you are using ? may be we can add on CI/CD



Sharon Brizinov @sean007 · 10 months ago

Author

Contributor

Looks good. I'll join. I think it could be much easier to setup a channel in a direct messaging platform such as Slack/Discord. I'll raise this on the dev den.

Regarding the fuzzer - I'm mostly using libfuzzer but I'm doing a lot of manual work on top of it to make sure we get full coverage. In addition, I'm going over Wireshark code and manually building crafted packets to reach interesting code flows to trigger a potential vulns.

Edited by [Sharon Brizinov](#) 10 months ago



Alexis La Goutte @alagoutte · 10 months ago

Developer

there is some plan about Slack/Discord but not yet available...

ok for libfuzzer, it can be possible to automatize some stuff ?



Graham Bloice @graham.bloice · 10 months ago

Developer

There is a Slack workspace, "[wireshark.slack.com](#)" but I think it's a closed group or whatever the Slack terminology for that is.



Sharon Brizinov @sean007 · 10 months ago

Author

Contributor

As requested I opened a new Issue with all the warning I could possibly find. I did both manual and automation testing to try to reach all assertion failures in all the dissectors.

<https://gitlab.com/wireshark/wireshark/-/issues/17890>

[@alagoutte](#) IMO the important aspect is to go over all the corpuses I found before any stable release, and obviously enrich it all the time. I will raise this in the upcoming dev den.

[@graham.bloice](#) how can I get an invite to that Slack workspace ?

Edited by [Sharon Brizinov](#) 10 months ago



Graham Bloice @graham.bloice · 10 months ago

Developer

[@geraldcombs](#) Is the [wireshark.slack.workspace](#) only for core devs, I'm not sure.



Alexis La Goutte @alagoutte · 10 months ago

Developer

it is for -core only



Sharon Brizinov @sean007 · 10 months ago

Author

Contributor

[@alagoutte](#) can you add me to a specific channel to discuss security aspects of Wireshark? I have some ideas which I want to share & collaborate.



Gerald Combs @geraldcombs · 10 months ago

Owner

[@sean007](#) were you looking for a general "security" channel or one specific to the issues here?



[Sharon Brizinov](#) @sean007 · 10 months ago

Author

Contributor

[@geraldcombs](#) general one 🤔



[Gerald Combs](#) @geraldcombs · 10 months ago

Owner

OK, we have a Discord channel set up and you can join at <https://discord.gg/RY2n4V3Z>. Note that the link will expire in 7 days.

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



[Jaap Keuter](#) @JaapKeuter · 10 months ago

Developer

For the `../epan/tvbuff_lznt1.c:135:10:` case in SMB, would it make sense to make the following change:

```
static gboolean
do_uncompress(tvbuff_t *tvb, int offset, int in_size, wmem_array_t *obuf)
{
    int in_off = 0;
    guint32 header, length, i;
    gboolean ok;

    if (!tvb)
        return FALSE;

-   if (in_size > MAX_INPUT_SIZE)
+   if (!in_size || in_size > MAX_INPUT_SIZE)
        return FALSE;
```

In order to prevent an empty TVB to be created.

This then results in a proper dissection output:

```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Compression Transform Header
    ProtocolId: 0xfc534d42
    OriginalSize: 0
    CompressionAlgorithm: LZNT1 (0x0001)
    Flags: None (0x0000)
    Offset: 0x00000000
    Compressed SMB3 data
      CompressedData: <MISSING>
```



[Sharon Brizinov](#) @sean007 · 10 months ago

Author

Contributor

I think it's a good idea. It will solve potential future issues too when decompressing `lznt1` stream

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



[Jaap Keuter](#) marked the checklist item **TCP** as completed 10 months ago



[Jaap Keuter](#) marked the checklist item **JXTA** as completed 10 months ago



[Jaap Keuter](#) mentioned in merge request [!5947 \(merged\)](#) 10 months ago



[Jaap Keuter](#) marked the checklist item **SMB2 (SMB3)** as completed 10 months ago



[Gerald Combs](#) mentioned in merge request [!6015 \(merged\)](#) 10 months ago



[Gerald Combs](#) mentioned in merge request [!6016 \(merged\)](#) 10 months ago



Gerald Combs @geraldcombs · 10 months ago

Owner

Backport status:

Master MR	Master Commit	3.6 MR	3.6 Commit	3.4 MR	3.4 Commit
!5899 (merged)	1b461768	!6012 (merged)	9544ddb2	!6011 (merged)	7a17991d
!5900 (merged)	5ee31161	!6013 (merged)	e66bcc2a	!6014 (merged)	2a4ac6e4
!5922 (merged)	f7b6ebcc	!6015 (merged)	cf7f98ca	!6016 (merged)	95242073
!5928 (merged)	3c4d2a28	!6017 (merged)	a2eb6dc5	!6018 (merged)	e32f54a5
!5947 (merged)	e1f025d9	!6019 (merged)	2fa40b82	!6020 (merged)	8e93fe67
!6055 (merged)	1fd18538	!6127 (merged)	30b84545	!6128 (merged)	62fae896

Edited by [Gerald Combs](#) 9 months ago



[Dario Lombardo](#) mentioned in commit [cf7f98ca](#) 9 months ago



[Gerald Combs](#) mentioned in merge request [!6055 \(merged\)](#) 9 months ago



[Sharon Brizinov](#) marked the checklist item **CSN1 (X2AP)** as completed 9 months ago



Sharon Brizinov @sean007 · 9 months ago

Author

Contributor

Amazing



[Dario Lombardo](#) mentioned in commit [95242073](#) 9 months ago



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



[Gerald Combs](#) mentioned in merge request [!6127 \(merged\)](#) 9 months ago



[Gerald Combs](#) mentioned in merge request [!6128 \(merged\)](#) 9 months ago



[Gerald Combs](#) mentioned in commit [30b84545](#) 9 months ago



[Gerald Combs](#) mentioned in commit [62fae896](#) 9 months ago



[Gerald Combs](#) closed 9 months ago



Gerald Combs @geraldcombs · 9 months ago

Owner

CSN1 (X2AP)

This has been assigned CVE-2022-0582.



[Gerald Combs](#) mentioned in merge request [!6265 \(merged\)](#) 9 months ago

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