Tvheadend - Bug #4328

Crash - heap-use-after-free

2017-04-22 14:55 - C K

Status:	Invalid	**Start date:**	2017-04-22
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Found in version:	4.1-2539~g496a58e42	**Affected Versions:**	

Description

Hi, tvheadend just crashed with this message:

```
    #9 0x562810e8fc41  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x72ec41)
    #10 0x562810e79c85  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x718c85)
    #11 0x562810e5e21a  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x6fd21a)
    #12 0x7fe5e558b493  (/lib/x86_64-linux-gnu/libpthread.so.0+0x7493)

previously allocated by thread T788 (tvh:tcp-start) here:
    #0 0x562810ddc9c8  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x67b9c8)
    #1 0x562810f78f1c  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x817f1c)
    #2 0x562810e64d0a  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x703d0a)
    #3 0x562810e61bdd  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x700bdd)
    #4 0x562810e8940d  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x72840d)
    #5 0x562810e9acd3  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x739cd3)
    #6 0x562810e99245  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x738245)
    #7 0x562810e98f2a  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x737f2a)
    #8 0x562810e8f630  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x72e630)
    #9 0x562810e8d8fa  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x72c8fa)
    #10 0x562810e8fc41  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x72ec41)
    #11 0x562810e79c85  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x718c85)
    #12 0x562810e5e21a  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x6fd21a)
    #13 0x7fe5e558b493  (/lib/x86_64-linux-gnu/libpthread.so.0+0x7493)

Thread T788 (tvh:tcp-start) created by T13 (tvh:tcp-loop) here:
    #0 0x562810d51229  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x5f0229)
    #1 0x562810e5df11  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x6fcf11)
    #2 0x562810e7883c  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x71783c)
    #3 0x562810e5e21a  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x6fd21a)
    #4 0x7fe5e558b493  (/lib/x86_64-linux-gnu/libpthread.so.0+0x7493)

Thread T13 (tvh:tcp-loop) created by T0 here:
    #0 0x562810d51229  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x5f0229)
    #1 0x562810e5df11  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x6fcf11)
    #2 0x562810e7791a  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x71691a)
    #3 0x562810e1a50b  (/home/ts/workspace/tvheadend/build.linux/tvheadend+0x6b950b)
    #4 0x7fe5e35ab2b0  (/lib/x86_64-linux-gnu/libc.so.6+0x202b0)

SUMMARY: AddressSanitizer: heap-use-after-free (/home/ts/workspace/tvheadend/build.linux/tvheadend
+0x6040f6)
Shadow bytes around the buggy address:
  0x0c0480157f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fd fd
  0x0c0480157f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480157f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480157f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480157f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c0480157f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fd]fd
  0x0c0480157f60: fa fa fa fa fa fa 00 05 fa fa fa fa fa fa fa fa
  0x0c0480157f70: fa fa fa fa fa fa 00 03 fa fa fa fa fa fa fa fa
  0x0c0480157f80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480157f90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa 00 00
  0x0c0480157fa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa 00 00
```

```
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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==4721==ABORTING
```

History

#1 - 2017-04-22 17:29 - Jaroslav Kysela

https://tvheadend.org/projects/tvheadend/wiki/Debugging#clang - pls, provide symbolic names

#2 - 2017-04-25 11:26 - C K

Please close this, can't confirm and i debugged wrong. Will create a new bug if it happens again.

#3 - 2017-04-25 18:11 - Jaroslav Kysela

- Status changed from New to Invalid