verf1sh / Poc Public

Code Issues Pull requests Actions Projects Security Insights

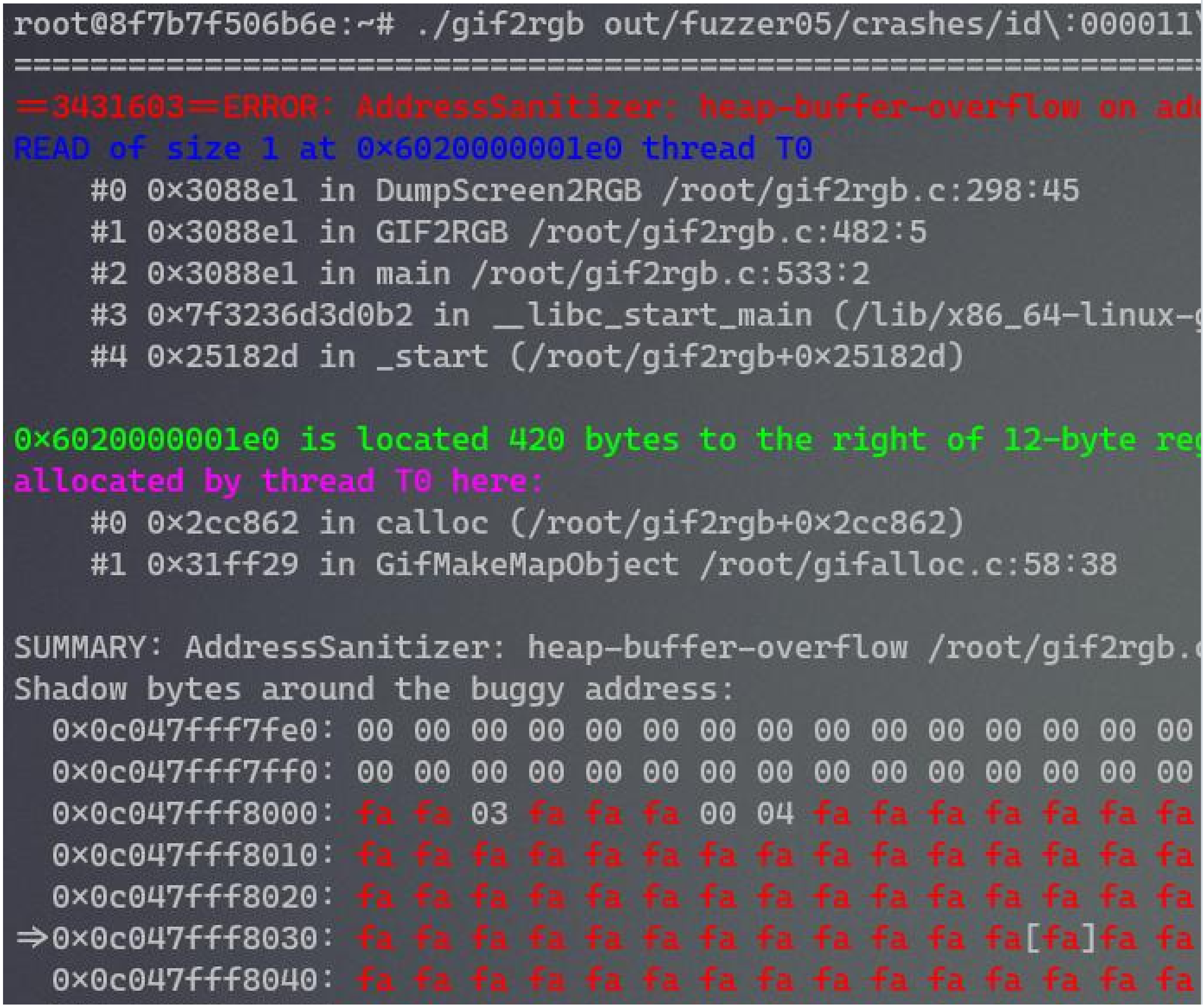
master

Poc / asan_report_giflib.png

verf1sh Add files via upload History

1 contributor

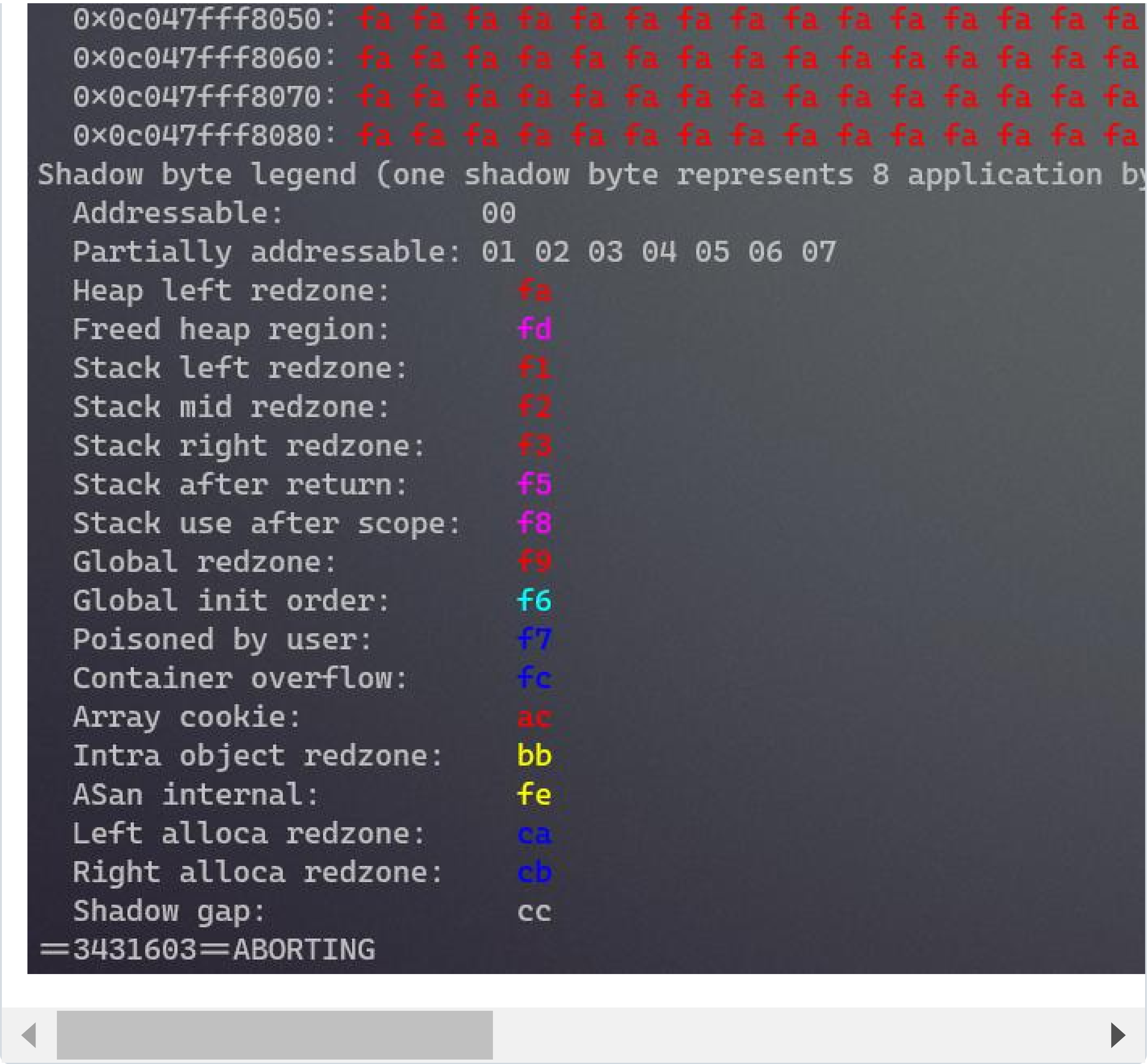
2 MB



```
root@8f7b7f506b6e:~# ./gif2rgb out/fuzzer05/crashes/id\:000011
=================================================================
==3431603==ERROR: AddressSanitizer: heap-buffer-overflow on add
READ of size 1 at 0x6020000001e0 thread T0
    #0 0x3088e1 in DumpScreen2RGB /root/gif2rgb.c:298:45
    #1 0x3088e1 in GIF2RGB /root/gif2rgb.c:482:5
    #2 0x3088e1 in main /root/gif2rgb.c:533:2
    #3 0x7f3236d3d0b2 in __libc_start_main (/lib/x86_64-linux-g
    #4 0x25182d in _start (/root/gif2rgb+0x25182d)

0x6020000001e0 is located 420 bytes to the right of 12-byte reg
allocated by thread T0 here:
    #0 0x2cc862 in calloc (/root/gif2rgb+0x2cc862)
    #1 0x31ff29 in GifMakeMapObject /root/gifalloc.c:58:38

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/gif2rgb.c
Shadow bytes around the buggy address:
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 03 fa fa fa 00 04 fa fa fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```



```
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application by
  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
==3431603==ABORTING
```