R

# otfcc's issue Reference

% repo link

https://github.com/caryll/otfcc

- % Requesting CVE id
- % command to reproduce:

shell

- 1 ./otfccbuild -O3 -q --force-cid [sample file] -o /dev/null
- % catalogue 1: Vulnerability type heap buffer overflow
- % sample file :
- ttps://drive.google.com/file/d/1m8K86hpdDFDC2KcbD2QQ3yAD2zpBrA2f/view?usp=sharing

43

44

45

Global redzone:

Global init order:

Poisoned by user:

f9

f6

f7

gradle ==100398==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000044b at 2 READ of size 4294967295 at 0x61200000044b thread T0 3 #0 0x4adb11 in asan memcpy (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+ #1 0x6b53ed (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed) 4 #2 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99) 5 6 #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa) 7 #4 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe) #5 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710) 8 #6 0x7f6a7f4b6c86 in \_\_libc\_start\_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/ 9 10 #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549) 11 0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6 12 allocated by thread T0 here: 13 14 #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5) 15 #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe) 16 17 #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710) #4 0x7f6a7f4b6c86 in \_\_libc\_start\_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/ 18 19 20 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release 21 Shadow bytes around the buggy address: 0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00 22 23 0x0c247fff8050: 00 00 00 00 00 00 00 00 00 fa fa fa fa fa 24 0x0c247fff8060: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00 25 26 =>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa 27 28 29 30 31 32 33 Shadow byte legend (one shadow byte represents 8 application bytes): 34 Addressable: 00 35 Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: 36 fa Freed heap region: fd 37 Stack left redzone: f1 38 39 Stack mid redzone: f2 Stack right redzone: f3 40 Stack after return: f5 41 Stack use after scope: f8 42

```
Container overflow:
46
                                 fc
      Array cookie:
47
                                 ac
      Intra object redzone:
48
                                 bb
      ASan internal:
49
                                 fe
       Left alloca redzone:
50
                                 ca
       Right alloca redzone:
51
                                 cb
52
       Shadow gap:
                                 СС
53
    ==100398==ABORTING
```

https://drive.google.com/file/d/1BZ\_T5C1cPfYgvuelBJ8vu45zZcSNhJAt/view?usp=sharing

```
gradle
   ______
2
   ==111746==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000044b at
   READ of size 1 at 0x61200000044b thread T0
3
      #0 0x6b558f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b558f)
4
5
      #1 0x6b6bf3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6bf3)
      #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
6
      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
7
      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
8
      #5 0x7ff49f52ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11
   0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
12
   allocated by thread T0 here:
13
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
14
      #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
15
16
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
17
      #4 0x7ff49f52ec86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
18
19
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
20
   Shadow bytes around the buggy address:
21
22
     0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
23
     0x0c247fff8050: 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
24
     0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
25
     26
27
   =>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
28
     29
     30
     31
```

```
32
    Shadow byte legend (one shadow byte represents 8 application bytes):
33
      Addressable:
34
                           00
      Partially addressable: 01 02 03 04 05 06 07
35
      Heap left redzone:
36
                             fa
37
      Freed heap region:
                             fd
      Stack left redzone:
38
                             f1
      Stack mid redzone:
39
                             f2
      Stack right redzone:
40
                             f3
      Stack after return:
                             f5
41
      Stack use after scope:
42
                             f8
      Global redzone:
                             f9
43
     Global init order:
                             f6
44
      Poisoned by user:
                             f7
45
      Container overflow:
46
                             fc
     Array cookie:
47
                             ac
      Intra object redzone:
48
                             bb
49
      ASan internal:
                             fe
      Left alloca redzone:
50
                             ca
      Right alloca redzone:
51
                             cb
52
      Shadow gap:
                             СС
    ==111746==ABORTING
53
```

https://drive.google.com/file/d/1Tm4VQLzEsHYm-VZm-8S3li854wnKpgby/view?usp=sharing

```
gradle
                                                                                  R
1
    ______
2
    ==117024==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000000832 at
    READ of size 1 at 0x616000000832 thread T0
3
        #0 0x6e7e3d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e7e3d)
4
5
        #1 0x5eb58a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb58a)
        #2 0x4fe227 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
6
7
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #4 0x7fcd6ac0dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
    0x616000000832 is located 680 bytes to the right of 522-byte region [0x616000000380,0
11
    allocated by thread T0 here:
12
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
        #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
14
15
        #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
        #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
        #4 0x7fcd6ac0dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
17
```

```
18
  SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
19
20
  Shadow bytes around the buggy address:
   0x0c2c7fff80b0: 00 02 fa fa
21
   22
   23
   24
   25
  26
27
   28
   29
   30
   31
  Shadow byte legend (one shadow byte represents 8 application bytes):
32
   Addressable:
33
                00
   Partially addressable: 01 02 03 04 05 06 07
34
35
   Heap left redzone:
                  fa
                  fd
36
   Freed heap region:
   Stack left redzone:
                  f1
37
   Stack mid redzone:
                  f2
38
39
   Stack right redzone:
                  f3
   Stack after return:
40
                  f5
   Stack use after scope:
                  f8
41
   Global redzone:
                  f9
42
   Global init order:
                  f6
43
44
   Poisoned by user:
                  f7
   Container overflow:
                  fc
45
46
   Array cookie:
                  ac
   Intra object redzone:
47
                  hh
   ASan internal:
                  fe
48
   Left alloca redzone:
49
                  ca
   Right alloca redzone:
50
                  ch
   Shadow gap:
51
                  CC
52
  ==117024==ABORTING
```

https://drive.google.com/file/d/1u3986achSUKMuFQ8qdE8aLV4ypy-SDnz/view?usp=sharing

```
5
      #2 0x4fe227 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6
7
      #4 0x7fdfdc8c8c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
      #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
   0x616000000837 is located 685 bytes to the right of 522-byte region [0x616000000380,0
10
11
   allocated by thread T0 here:
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
      #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13
14
      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
15
      #4 0x7fdfdc8c8c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
17
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
18
   Shadow bytes around the buggy address:
19
    0x0c2c7fff80b0: 00 02 fa fa
20
    21
    22
    23
    24
   25
    26
    27
    28
    29
    30
   Shadow byte legend (one shadow byte represents 8 application bytes):
31
    Addressable:
32
                     00
33
    Partially addressable: 01 02 03 04 05 06 07
    Heap left redzone:
34
                      fa
    Freed heap region:
                      fd
35
    Stack left redzone:
                      f1
36
    Stack mid redzone:
                      f2
37
    Stack right redzone:
                      f3
38
    Stack after return:
                      f5
39
    Stack use after scope:
40
                      f8
    Global redzone:
                      f9
41
    Global init order:
                      f6
42
    Poisoned by user:
43
                      f7
44
    Container overflow:
                      fc
    Array cookie:
45
                      ac
    Intra object redzone:
                      bb
46
    ASan internal:
                      fe
47
    Left alloca redzone:
48
                      ca
    Right alloca redzone:
49
                      cb
    Shadow gap:
50
                      CC
   ==106716==ABORTING
51
```

https://drive.google.com/file/d/1UQx\_BSWEGga18psFBjhkusjFvDA0ER\_Z/view?usp=sharing

```
gradle
1
   ______
2
   ==107908==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000005cb at
3
   READ of size 1 at 0x6120000005cb thread T0
4
      #0 0x6b5567 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b5567)
5
      #1 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
      #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
6
7
      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
8
      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
      #5 0x7fc74767cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11
12
   0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
   allocated by thread T0 here:
13
14
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
15
      #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
16
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
17
      #4 0x7fc74767cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
18
19
20
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
   Shadow bytes around the buggy address:
21
22
     0x0c247fff8060: fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
23
     24
     0x0c247fff8090: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
25
26
     27
   =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa
     28
29
     30
     31
     32
   Shadow byte legend (one shadow byte represents 8 application bytes):
33
34
     Addressable:
                      00
     Partially addressable: 01 02 03 04 05 06 07
35
    Heap left redzone:
36
                        fa
    Freed heap region:
                        fd
37
    Stack left redzone:
                        f1
38
    Stack mid redzone:
                        f2
39
     Stack right redzone:
                        f3
40
    Stack after return:
                        f5
41
```

```
Stack use after scope:
42
                                 f8
       Global redzone:
                                 f9
43
      Global init order:
                                 f6
44
45
      Poisoned by user:
                                 f7
      Container overflow:
                                 fc
46
      Array cookie:
47
                                 ac
48
       Intra object redzone:
                                 bb
      ASan internal:
49
                                 fe
      Left alloca redzone:
50
                                 ca
       Right alloca redzone:
51
                                 cb
52
       Shadow gap:
                                 CC
    ==107908==ABORTING
53
```

https://drive.google.com/file/d/1CdfTd5Emf\_jDRLv1z64W5Rm3O1Q1JTyQ/view?usp=sharing

```
gradle
                                                                             R
    ==108759==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000000616 at
    READ of size 1 at 0x612000000616 thread T0
2
       #0 0x6b064d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b064d)
3
       #1 0x6b256a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
4
5
       #2 0x6b74c0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
       #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
6
       #4 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
7
       #5 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
8
       #6 0x7f93b614bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9
       #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11
12
    0x612000000616 is located 75 bytes to the right of 267-byte region [0x6120000004c0,0x
    allocated by thread T0 here:
13
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
14
       #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
15
       #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
16
       #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
17
       #4 0x7f93b614bc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
18
19
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
20
    Shadow bytes around the buggy address:
21
22
      23
      24
     0x0c247fff8090: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
25
     0x0c247fff80b0: 00 00 00 00 00 00 00 00 03 fa fa fa fa fa fa
26
    =>0x0c247fff80c0: fa fa[fa]fa fa fa
27
```

```
28
    29
30
    31
    32
33
   Shadow byte legend (one shadow byte represents 8 application bytes):
34
    Addressable:
                    00
35
    Partially addressable: 01 02 03 04 05 06 07
    Heap left redzone:
                     fa
36
    Freed heap region:
                     fd
37
    Stack left redzone:
38
                     f1
    Stack mid redzone:
                     f2
39
    Stack right redzone:
                     f3
40
    Stack after return:
                     f5
41
    Stack use after scope:
                     f8
42
    Global redzone:
                     f9
43
    Global init order:
                     f6
44
45
    Poisoned by user:
                     f7
    Container overflow:
                     fc
46
    Array cookie:
47
                     ac
    Intra object redzone:
48
                     bb
    ASan internal:
49
                     fe
    Left alloca redzone:
50
                     ca
    Right alloca redzone:
51
                     cb
52
    Shadow gap:
                     CC
   ==108759==ABORTING
53
```

https://drive.google.com/file/d/1e1fXghAuLNy-1-nsPoOX8XeFIGkifkML/view?usp=sharing

```
R
gradle
    ==109163==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000008bd at
 1
    READ of size 1 at 0x6120000008bd thread T0
 2
 3
        #0 0x6adb1e (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6adb1e)
        #1 0x6b71de (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b71de)
 4
        #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
 5
        #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
 6
        #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
 7
        #5 0x7f199d870c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
 8
        #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
 9
10
11
    0x6120000008bd is located 754 bytes to the right of 267-byte region [0x6120000004c0,0
    allocated by thread T0 here:
12
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
```

```
#1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
14
     #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
15
     #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
16
     #4 0x7f199d870c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
17
18
19
  SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
  Shadow bytes around the buggy address:
20
    21
    22
23
    24
    25
  26
27
    28
    29
    30
    31
  Shadow byte legend (one shadow byte represents 8 application bytes):
32
    Addressable:
                  00
33
    Partially addressable: 01 02 03 04 05 06 07
34
   Heap left redzone:
35
                   fa
    Freed heap region:
                   fd
36
    Stack left redzone:
37
                   f1
    Stack mid redzone:
                   f2
38
   Stack right redzone:
                   f3
39
   Stack after return:
                   f5
40
   Stack use after scope:
                   f8
41
42
    Global redzone:
                   f9
   Global init order:
43
                   f6
    Poisoned by user:
                   f7
44
   Container overflow:
45
                   fc
   Array cookie:
46
                   ac
    Intra object redzone:
47
                   bb
   ASan internal:
                   fe
48
    Left alloca redzone:
49
                   ca
    Right alloca redzone:
50
                   cb
    Shadow gap:
51
                   CC
  ==109163==ABORTING
52
```

https://drive.google.com/file/d/15zgWcgkig0fr36a7wOgurSltd1rg9n0\_/view?usp=sharing





```
1
   ==109553==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000078a6 at
2
   READ of size 1 at 0x6160000078a6 thread T0
3
     #0 0x6e20a0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e20a0)
     #1 0x5eb5ec (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb5ec)
4
     #2 0x4fe227 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
5
     #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6
7
     #4 0x7f2da0c05c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
     #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
   Address 0x6160000078a6 is a wild pointer.
10
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
11
   Shadow bytes around the buggy address:
12
    13
    14
    15
    16
    17
   =>0x0c2c7fff8f10: fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa fa
18
    19
    20
    21
    22
    23
24
   Shadow byte legend (one shadow byte represents 8 application bytes):
25
    Addressable:
                    00
    Partially addressable: 01 02 03 04 05 06 07
26
    Heap left redzone:
27
                     fa
    Freed heap region:
                     fd
28
29
    Stack left redzone:
                     f1
    Stack mid redzone:
                     f2
30
    Stack right redzone:
                     f3
31
32
    Stack after return:
                     f5
33
    Stack use after scope: f8
    Global redzone:
                     f9
34
    Global init order:
                     f6
35
    Poisoned by user:
36
                     f7
    Container overflow:
37
                     fc
    Array cookie:
38
                      ac
39
    Intra object redzone:
                     bb
    ASan internal:
                     fe
40
    Left alloca redzone:
41
                      ca
    Right alloca redzone:
42
                      cb
43
    Shadow gap:
                      CC
   ==109553==ABORTING
44
```

Intra object redzone:

bb

45

gradle R ==109939==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000001d6 at 2 READ of size 1 at 0x6020000001d6 thread T0 3 #0 0x5e15d8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5e15d8) #1 0x4fe1e2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe1e2) 4 #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710) 5 6 #3 0x7f502f9c0c86 in \_\_libc\_start\_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/ 7 #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549) 8 9 0x6020000001d6 is located 0 bytes to the right of 6-byte region [0x6020000001d0,0x602 10 allocated by thread T0 here: #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd 11 #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f) 12 #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31) 13 #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc) 14 #4 0x7f502f9c0c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/ 15 16 17 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release Shadow bytes around the buggy address: 18 19 20 21 0x0c047fff8000: fa fa 00 00 fa fa 00 03 fa fa fd fa fa fa 00 03 0x0c047fff8010: fa fa fd fa fa fa 00 00 fa fa fd fa fa fd fa 22 0x0c047fff8020: fa fa fd fa fa fd fa fa fd fa fa fd fa 23 =>0x0c047fff8030: fa fa 04 fa fa fa 00 fa fa fa[06]fa fa fa fd fa 24 0x0c047fff8040: fa fa fd fa fa fd fa fa fa fd fa fa fa fd fa 25 0x0c047fff8050: fa fa fd fa fa fd fa fa fa fd fa fa fa fd fa 26 0x0c047fff8060: fa fa fd fa fa fa 00 00 fa fa fa fa fa fa fa 27 28 29 Shadow byte legend (one shadow byte represents 8 application bytes): 30 31 Addressable: 00 32 Partially addressable: 01 02 03 04 05 06 07 fa Heap left redzone: 33 34 Freed heap region: fd Stack left redzone: 35 f1 Stack mid redzone: f2 36 Stack right redzone: f3 37 Stack after return: f5 38 39 Stack use after scope: f8 Global redzone: f9 40 Global init order: f6 41 Poisoned by user: f7 42 43 Container overflow: fc **4**4 Array cookie: ac

```
46 ASan internal: fe
47 Left alloca redzone: ca
48 Right alloca redzone: cb
49 Shadow gap: cc
50 ==109939==ABORTING
```

https://drive.google.com/file/d/1Gtp0aHRoRq5pDa73jXMcBZIIsu2dCs7B/view?usp=sharing

```
R
gradle
   ==110431==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
   READ of size 1 at 0x61200000044b thread T0
2
3
      #0 0x6b559f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b559f)
4
      #1 0x6b6d86 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6d86)
      #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
5
      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
7
      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
8
      #5 0x7f17f472ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
11
   0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
   allocated by thread T0 here:
12
13
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
      #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
14
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
15
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
16
      #4 0x7f17f472ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
17
18
19
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
   Shadow bytes around the buggy address:
20
     0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
21
     22
     0x0c247fff8050: 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
23
     0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
24
     25
26
   =>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
     27
     28
     29
     30
     31
32
   Shadow byte legend (one shadow byte represents 8 application bytes):
     Addressable:
33
     Partially addressable: 01 02 03 04 05 06 07
34
```

```
Heap left redzone:
35
                                 fa
       Freed heap region:
                                 fd
36
37
       Stack left redzone:
                                 f1
38
       Stack mid redzone:
                                 f2
       Stack right redzone:
39
                                 f3
       Stack after return:
                                 f5
40
41
       Stack use after scope:
                                 f8
42
       Global redzone:
                                 f9
       Global init order:
43
                                 f6
       Poisoned by user:
                                 f7
44
45
      Container overflow:
                                 fc
       Array cookie:
46
                                 ac
       Intra object redzone:
47
                                 bb
      ASan internal:
                                 fe
48
       Left alloca redzone:
49
                                 ca
50
       Right alloca redzone:
                                 cb
51
       Shadow gap:
                                 СС
52
    ==110431==ABORTING
```

https://drive.google.com/file/d/1COw6yyp8w99fEVhoeBz9mBw4h0\_aZi\_n/view?usp=sharing

```
gradle
                                                                                       R
    ==110920==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000005cb at
 1
    READ of size 1 at 0x6120000005cb thread T0
 2
        #0 0x6b0b2c (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0b2c)
 3
        #1 0x6b256a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
 4
        #2 0x6b74c0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
 5
        #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
 6
 7
        #4 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
 8
        #5 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
 9
        #6 0x7f857d9cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
        #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11
12
    0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
    allocated by thread T0 here:
13
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
14
15
        #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
        #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
16
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
17
        #4 0x7f857d9cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
18
19
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
20
    Shadow bytes around the buggy address:
21
```

```
0x0c247fff8060: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
22
    23
    24
25
    0x0c247fff8090: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
    26
27
  =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
28
    29
    30
    31
    32
  Shadow byte legend (one shadow byte represents 8 application bytes):
33
34
    Addressable:
                  00
    Partially addressable: 01 02 03 04 05 06 07
35
    Heap left redzone:
36
                    fa
    Freed heap region:
                    fd
37
    Stack left redzone:
                    f1
38
39
    Stack mid redzone:
                    f2
    Stack right redzone:
                    f3
40
    Stack after return:
                    f5
41
    Stack use after scope:
42
                    f8
    Global redzone:
                    f9
43
    Global init order:
44
                    f6
    Poisoned by user:
                    f7
45
    Container overflow:
                    fc
46
    Array cookie:
47
                    ac
    Intra object redzone:
48
                    bb
    ASan internal:
                    fe
49
    Left alloca redzone:
50
                    ca
    Right alloca redzone:
51
                    ch
    Shadow gap:
52
                    CC
  ==110920==ABORTING
53
```

https://drive.google.com/file/d/1GzEsD9U0bzjg9\_Wi2i4f8yVTLA-gzgd8/view?usp=sharing

```
gradle

1 ==112565==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x608000000178 at
2 READ of size 1 at 0x608000000178 thread T0
3 #0 0x6b05aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05aa)
4 #1 0x6b99ca (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
5 #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
6 #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
7 #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
```

```
8
      #5 0x7f1fc338fc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
   0x608000000178 is located 0 bytes to the right of 88-byte region [0x608000000120,0x60
11
12
   allocated by thread T0 here:
13
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
14
      #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
15
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
   Shadow bytes around the buggy address:
17
18
     19
     20
    0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
21
    0x0c107fff8010: fa fa fa fd fd
22
   =>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 [fa]
23
     24
    25
    26
    27
     28
   Shadow byte legend (one shadow byte represents 8 application bytes):
29
    Addressable:
30
                     00
    Partially addressable: 01 02 03 04 05 06 07
31
32
    Heap left redzone:
                       fa
    Freed heap region:
                       fd
33
    Stack left redzone:
34
                       f1
35
    Stack mid redzone:
                       f2
36
    Stack right redzone:
                       f3
    Stack after return:
                       f5
37
38
    Stack use after scope:
                       f8
    Global redzone:
                       f9
39
    Global init order:
                       f6
40
    Poisoned by user:
                       f7
41
    Container overflow:
42
                       fc
    Array cookie:
43
                       ac
    Intra object redzone:
44
                       bb
    ASan internal:
                       fe
45
    Left alloca redzone:
46
                       ca
47
    Right alloca redzone:
                       cb
48
    Shadow gap:
                       CC
49
   ==112565==ABORTING
```

https://drive.google.com/file/d/1is411Z2h-rU5Yq4rHBJhw2c7Cpi1C7U4/view?usp=sharing



```
1
   ==112975==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000005cb at
   READ of size 1 at 0x6120000005cb thread T0
2
3
      #0 0x6b55af (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b55af)
      #1 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
4
      #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
5
      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
7
      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
      #5 0x7fc4b3c13c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
   0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
11
12
   allocated by thread T0 here:
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
14
      #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
15
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
16
      #4 0x7fc4b3c13c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
17
18
19
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
   Shadow bytes around the buggy address:
20
     0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
21
     22
     23
     0x0c247fff8090: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
24
25
     =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa
26
27
     28
     29
     30
     31
   Shadow byte legend (one shadow byte represents 8 application bytes):
32
     Addressable:
33
                       00
     Partially addressable: 01 02 03 04 05 06 07
34
     Heap left redzone:
                         fa
35
36
     Freed heap region:
                         fd
     Stack left redzone:
                         f1
37
     Stack mid redzone:
                         f2
38
     Stack right redzone:
                         f3
39
     Stack after return:
40
                         f5
     Stack use after scope:
41
                         f8
     Global redzone:
                         f9
42
     Global init order:
43
                         f6
     Poisoned by user:
44
                         f7
     Container overflow:
45
                         fc
     Array cookie:
46
                         ac
47
     Intra object redzone:
                         bb
```

```
48 ASan internal: fe
49 Left alloca redzone: ca
50 Right alloca redzone: cb
51 Shadow gap: cc
52 ==112975==ABORTING
```

https://drive.google.com/file/d/1\_KAm-VI\_nxWaT2nlyEraZSU9lfgclzF0/view?usp=sharing

```
gradle
                                                             R
   ==113407==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f18b85fb808 at
1
   READ of size 8 at 0x7f18b85fb808 thread T0
2
      #0 0x6c08a6 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c08a6)
3
      #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
4
5
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6
      #4 0x7f18bbbcac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
7
      #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
   0x7f18b85fb808 is located 8 bytes to the right of 1048576-byte region [0x7f18b84fb800
10
11
   allocated by thread T0 here:
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
      #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
13
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
14
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
15
      #4 0x7f18bbbcac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
17
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
18
   Shadow bytes around the buggy address:
19
    20
21
    22
    23
    24
    =>0x0fe3970b7700: fa[fa]fa fa fa
25
    26
    27
    28
    29
    30
31
   Shadow byte legend (one shadow byte represents 8 application bytes):
    Addressable:
32
    Partially addressable: 01 02 03 04 05 06 07
33
34
                      fa
    Heap left redzone:
```

```
Freed heap region:
                                 fd
35
      Stack left redzone:
                                 f1
36
37
      Stack mid redzone:
                                 f2
38
      Stack right redzone:
                                 f3
       Stack after return:
39
                                 f5
      Stack use after scope:
40
                                 f8
41
      Global redzone:
                                 f9
      Global init order:
42
                                 f6
      Poisoned by user:
43
                                 f7
      Container overflow:
                                 fc
44
      Array cookie:
45
                                 ac
      Intra object redzone:
46
                                 bb
      ASan internal:
47
                                 fe
      Left alloca redzone:
48
                                 ca
      Right alloca redzone:
49
                                 cb
50
      Shadow gap:
                                 CC
    ==113407==ABORTING
51
```

https://drive.google.com/file/d/15eF0Yoha7rRLNmRadlOjd0kGzqVfD8M6/view?usp=sharing

```
gradle
                                                                                R
1
    ______
    ==113825==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
2
3
    READ of size 1 at 0x6120000005cb thread T0
       #0 0x6b84b1 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b84b1)
4
5
       #1 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
       #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
7
       #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
       #4 0x7f8d208dcc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
       #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
    0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
11
    allocated by thread T0 here:
12
13
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
14
       #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
       #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
15
       #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
16
       #4 0x7f8d208dcc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
17
18
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
19
20
    Shadow bytes around the buggy address:
      0x0c247fff8060: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
21
      22
```

```
23
    0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
24
25
    =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa
26
    27
    28
    29
    30
    31
  Shadow byte legend (one shadow byte represents 8 application bytes):
32
33
    Addressable:
                   00
    Partially addressable: 01 02 03 04 05 06 07
34
35
    Heap left redzone:
                    fa
    Freed heap region:
                    fd
36
    Stack left redzone:
                    f1
37
    Stack mid redzone:
                    f2
38
    Stack right redzone:
39
                    f3
40
    Stack after return:
                    f5
    Stack use after scope:
                    f8
41
    Global redzone:
                    f9
42
    Global init order:
43
                    f6
    Poisoned by user:
                    f7
44
    Container overflow:
45
                    fc
    Array cookie:
46
                    ac
47
    Intra object redzone:
                    bb
    ASan internal:
48
                    fe
    Left alloca redzone:
49
                    ca
    Right alloca redzone:
50
                    cb
    Shadow gap:
51
                    CC
  ==113825==ABORTING
52
```

https://drive.google.com/file/d/18HcVR2pHDUKdmdG99VyD42CkDEp8vDfR/view?usp=sharing

```
gradle
                                                                                      R
    ==114199==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6030000000295 at
1
    READ of size 1 at 0x603000000295 thread T0
2
3
        #0 0x6b03b5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b03b5)
4
        #1 0x6b99ca (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
        #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
5
        #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
7
        #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #5 0x7f60e4d53c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
        #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
```

```
11
   0x603000000295 is located 0 bytes to the right of 21-byte region [0x603000000280,0x60
   allocated by thread T0 here:
12
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
       #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
14
15
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
   Shadow bytes around the buggy address:
17
     0x0c067fff8000: fa fa fd fd fd fa fa fd fd fd fa fa fa fd fd
18
     0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
19
     0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 fa fa fd fd fd fa
20
     0x0c067fff8030: fa fa fd fd fd fa fa fa 00 00 06 fa fa fd fd
21
     0x0c067fff8040: fd fa fa fa 00 00 00 fa fa fd fd fd fa fa fa
22
23
   =>0x0c067fff8050: 00 00[05]fa fa fa 00 00 00 fa fa fa fa fa fa fa
     24
25
     26
     27
     28
   Shadow byte legend (one shadow byte represents 8 application bytes):
29
     Addressable:
30
                        00
     Partially addressable: 01 02 03 04 05 06 07
31
     Heap left redzone:
32
                          fa
     Freed heap region:
33
                          fd
     Stack left redzone:
                          f1
34
     Stack mid redzone:
                          f2
35
     Stack right redzone:
                          f3
36
     Stack after return:
                          f5
37
38
     Stack use after scope:
                          f8
     Global redzone:
                          f9
39
     Global init order:
                          f6
40
     Poisoned by user:
                          f7
41
     Container overflow:
                          fc
42
     Array cookie:
43
                          ac
     Intra object redzone:
44
                          bb
     ASan internal:
45
                          fe
     Left alloca redzone:
46
                          ca
     Right alloca redzone:
47
                          cb
48
     Shadow gap:
                          CC
49
   ==114199==ABORTING
```

10

https://drive.google.com/file/d/19seFG4dOiRFEV7YwxZnUZNo4FRDr954E/view?usp=sharing



```
gradle
==114606==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x608000000178 at
2
   READ of size 1 at 0x608000000178 thread T0
3
      #0 0x6b04de (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b04de)
      #1 0x6b99ca (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
4
      #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
5
      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
7
      #5 0x7ff6deb1dc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
   0x608000000178 is located 0 bytes to the right of 88-byte region [0x608000000120,0x60
11
   allocated by thread T0 here:
12
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
      #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
14
15
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
   Shadow bytes around the buggy address:
17
     18
     19
     20
     0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
21
     0x0c107fff8010: fa fa fa fd fd
22
   =>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 [fa]
23
     24
     25
     26
     27
     28
   Shadow byte legend (one shadow byte represents 8 application bytes):
29
     Addressable:
                       00
30
     Partially addressable: 01 02 03 04 05 06 07
31
     Heap left redzone:
32
                         fa
     Freed heap region:
                         fd
33
     Stack left redzone:
                         f1
34
     Stack mid redzone:
                        f2
35
36
     Stack right redzone:
                         f3
     Stack after return:
                         f5
37
     Stack use after scope:
                        f8
38
     Global redzone:
                         f9
39
     Global init order:
40
                         f6
     Poisoned by user:
                         f7
41
42
     Container overflow:
                         fc
43
     Array cookie:
                         ac
     Intra object redzone:
44
                         bb
     ASan internal:
                         fe
45
     Left alloca redzone:
46
                         ca
     Right alloca redzone:
                         cb
```

```
48 Shadow gap: cc
49 ==114606==ABORTING
```

https://drive.google.com/file/d/1lh3\_DS7REltlSQaQyLkNDfoeC1APjlrC/view?usp=sharing

```
gradle
                                                                             R
    ==114999==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000519 at
2
    READ of size 1 at 0x602000000519 thread T0
3
       #0 0x6b0466 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0466)
       #1 0x6b99ca (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
4
       #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
5
       #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
7
       #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
       #5 0x7fc6f9544c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
       #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
    0x602000000519 is located 0 bytes to the right of 9-byte region [0x602000000510,0x602
11
    allocated by thread T0 here:
12
13
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
       #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
14
15
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
    Shadow bytes around the buggy address:
17
      0x0c047fff8050: fa fa fd fa fa fd fa fa fa fd fa fa fa fd fa
18
     0x0c047fff8060: fa fa fd fa fa fa 00 00 fa fa 07 fa fa fa 00 fa
19
     0x0c047fff8070: fa fa 07 fa fa fa 07 fa fa fa 07 fa fa fa 00 fa
20
21
     0x0c047fff8080: fa fa 07 fa fa fa 07 fa fa fa 00 00 fa fa 00 fa
     0x0c047fff8090: fa fa 05 fa fa fa 00 fa fa fa 00 00 fa fa 00 04
22
    =>0x0c047fff80a0: fa fa 00[01]fa fa 02 fa fa fa 00 01 fa fa 07 fa
23
     0x0c047fff80b0: fa fa 07 fa fa fa 00 fa fa fa 07 fa fa fa 00 00
24
25
     26
     27
      28
    Shadow byte legend (one shadow byte represents 8 application bytes):
29
     Addressable:
30
                          00
     Partially addressable: 01 02 03 04 05 06 07
31
32
     Heap left redzone:
                            fa
     Freed heap region:
                            fd
33
34
     Stack left redzone:
                            f1
     Stack mid redzone:
35
                            f2
     Stack right redzone:
                            f3
     Stack after return:
                            f5
37
```

```
Stack use after scope:
38
                                 f8
       Global redzone:
                                 f9
39
      Global init order:
                                 f6
40
41
      Poisoned by user:
                                 f7
      Container overflow:
42
                                 fc
      Array cookie:
43
                                 ac
44
      Intra object redzone:
                                 bb
      ASan internal:
45
                                 fe
      Left alloca redzone:
46
                                 ca
       Right alloca redzone:
47
                                 cb
48
       Shadow gap:
                                 CC
    ==114999==ABORTING
49
```

https://drive.google.com/file/d/1bk62xIR2SRqMNE9Q2IXDqDk54nGJZ6yl/view?usp=sharing

```
R
tap
1
   ==115405==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000000 at
   READ of size 1 at 0x607000000000 thread T0
2
       #0 0x617087 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x617087)
3
       #1 0x4feb66 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
4
5
       #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
       #3 0x7f93e83b7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
6
       #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
7
8
9
   0x6070000000e0 is located 0 bytes to the right of 80-byte region [0x607000000090,0x60
   allocated by thread T0 here:
10
11
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
       #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
       #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
13
       #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
14
       #4 0x7f93e83b7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
15
16
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17
18
   Shadow bytes around the buggy address:
     19
     20
     21
22
     23
     0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 04 fa fa fa
24
   =>0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 00 [fa]fa fa fa
25
     0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
     0x0c0e7fff8030: 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
26
     0x0c0e7fff8040: 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
27
```

```
0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd
28
       0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 fa
29
    Shadow byte legend (one shadow byte represents 8 application bytes):
30
31
       Addressable:
                              00
      Partially addressable: 01 02 03 04 05 06 07
32
33
      Heap left redzone:
                                fa
34
      Freed heap region:
                                fd
      Stack left redzone:
35
                                f1
      Stack mid redzone:
36
                                f2
      Stack right redzone:
                                f3
37
38
      Stack after return:
                                f5
39
      Stack use after scope:
                                f8
      Global redzone:
                                f9
40
      Global init order:
                                f6
41
      Poisoned by user:
                                f7
42
43
      Container overflow:
                                fc
      Array cookie:
44
                                ac
45
      Intra object redzone:
                                bb
      ASan internal:
46
                                fe
      Left alloca redzone:
47
                                ca
48
      Right alloca redzone:
                                cb
49
      Shadow gap:
                                CC
50
    ==115405==ABORTING
```

https://drive.google.com/file/d/1kagKNyCT9iVCtAN66-ZCSkst-MtlEJrh/view?usp=sharing

#### % crash info

16

```
gradle
                                                                                      R
    ==115805==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6140000003cd at
 1
    READ of size 1 at 0x6140000003cd thread T0
 2
 3
        #0 0x6b0d63 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0d63)
 4
        #1 0x6b256a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
        #2 0x6b74c0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
 5
        #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
 6
        #4 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
 7
        #5 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
 8
        #6 0x7f3e2b577c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
 9
        #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11
    0x6140000003cd is located 0 bytes to the right of 397-byte region [0x614000000240,0x6
12
    allocated by thread T0 here:
13
14
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
        #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
```

#2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)

```
17
     #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
18
     #4 0x7f3e2b577c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
19
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
20
21
   Shadow bytes around the buggy address:
22
    23
    0x0c287fff8030: 00 00 00 00 00 00 00 00 05 fa fa fa fa fa fa
24
    0x0c287fff8040: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
    25
    26
27
   =>0x0c287fff8070: 00 00 00 00 00 00 00 00 00[05]fa fa fa fa fa fa
28
    29
    30
    31
    32
   Shadow byte legend (one shadow byte represents 8 application bytes):
33
34
    Addressable:
    Partially addressable: 01 02 03 04 05 06 07
35
    Heap left redzone:
36
                      fa
37
    Freed heap region:
                      fd
    Stack left redzone:
                      f1
38
    Stack mid redzone:
39
                     f2
    Stack right redzone:
                      f3
40
    Stack after return:
                      f5
41
    Stack use after scope:
42
                     f8
    Global redzone:
                     f9
43
    Global init order:
                      f6
44
45
    Poisoned by user:
                      f7
    Container overflow:
46
                      fc
    Array cookie:
47
                      ac
    Intra object redzone:
48
                      bb
    ASan internal:
49
                      fe
    Left alloca redzone:
50
                      ca
    Right alloca redzone:
51
                      cb
52
    Shadow gap:
                      CC
53
   ==115805==ABORTING
```

https://drive.google.com/file/d/1WkYYIR-CFN8586TP9rHNCTfRI0GcW712/view?usp=sharing

#### % crash info

tap



==116203==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000000 at READ of size 1 at 0x6070000000000 thread TO

```
3
         #0 0x61731f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x61731f)
         #1 0x4feb66 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
  4
  5
         #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
         #3 0x7f448d7ccc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
  6
         #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
  7
  8
  9
     0x6070000000e0 is located 0 bytes to the right of 80-byte region [0x607000000090,0x60
     allocated by thread T0 here:
 10
         #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
 11
         #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
 12
 13
         #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
         #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
 14
         #4 0x7f448d7ccc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
 15
 16
     SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
 17
     Shadow bytes around the buggy address:
 18
       19
 20
       21
       22
       0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 04 fa fa fa
 23
     =>0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 [fa]fa fa fa
 24
 25
       0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
 26
       0x0c0e7fff8030: 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
       0x0c0e7fff8040: 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
 27
       0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd
 28
       0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 fa
 29
     Shadow byte legend (one shadow byte represents 8 application bytes):
 30
 31
       Addressable:
                            00
       Partially addressable: 01 02 03 04 05 06 07
 32
       Heap left redzone:
                             fa
 33
       Freed heap region:
 34
                             fd
       Stack left redzone:
                             f1
 35
       Stack mid redzone:
                             f2
 36
 37
       Stack right redzone:
                             f3
       Stack after return:
                             f5
 38
       Stack use after scope:
 39
                             f8
       Global redzone:
                             f9
 40
       Global init order:
 41
                             f6
 42
       Poisoned by user:
                             f7
       Container overflow:
 43
                             fc
       Array cookie:
 44
                             ac
       Intra object redzone:
                             bb
 45
       ASan internal:
 46
                             fe
       Left alloca redzone:
 47
                             ca
       Right alloca redzone:
 48
                             cb
       Shadow gap:
 49
                             \mathsf{CC}
$ 50
     ==116203==ABORTING
```

https://drive.google.com/file/d/1vwRpTYLgrh2zhc8eOwnavJOWCoGYXDFd/view?usp=sharing

```
gradle
                                                                               R
    ==116615==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000150 at
2
    READ of size 1 at 0x603000000150 thread T0
3
       #0 0x6171b2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6171b2)
4
       #1 0x4febdc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4febdc)
5
       #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
       #3 0x7f9e1c28bc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
6
7
       #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
    0x603000000150 is located 0 bytes to the right of 32-byte region [0x603000000130,0x60
    allocated by thread T0 here:
10
11
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
       #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13
       #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
       #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
14
15
       #4 0x7f9e1c28bc86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17
    Shadow bytes around the buggy address:
18
19
      20
      21
22
      0x0c067fff8000: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
23
      0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
    =>0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 [fa]fa 00 00 04 fa
24
25
      0x0c067fff8030: fa fa 00 00 00 00 fa fa fd fd fd fa fa fa fd fd
26
      0x0c067fff8040: fd fa fa fa 00 00 06 fa fa fd fd fd fa fa fa
27
      0x0c067fff8050: 00 00 00 fa fa fa fd fd fd fd fa fa 00 00 02 fa
      0x0c067fff8060: fa fa 00 00 02 fa fa fa 00 00 02 fa fa fa 00 00
28
29
      0x0c067fff8070: 02 fa fa fa 00 00 02 fa fa fa 00 00 02 fa fa fa
30
    Shadow byte legend (one shadow byte represents 8 application bytes):
      Addressable:
                           00
31
32
      Partially addressable: 01 02 03 04 05 06 07
33
     Heap left redzone:
                             fa
34
      Freed heap region:
                             fd
     Stack left redzone:
                            f1
35
     Stack mid redzone:
                            f2
36
     Stack right redzone:
                            f3
37
     Stack after return:
                             f5
38
     Stack use after scope:
                             f8
39
      Global redzone:
                             f9
40
     Global init order:
                             f6
41
```

```
Poisoned by user:
42
                                 f7
      Container overflow:
43
                                 fc
      Array cookie:
44
                                 ac
45
      Intra object redzone:
                                 bb
      ASan internal:
46
                                 fe
      Left alloca redzone:
47
                                 ca
48
       Right alloca redzone:
                                 cb
49
       Shadow gap:
                                 CC
    ==116615==ABORTING
50
```

https://drive.google.com/file/d/1 PTp8qpryF4AwtMnMxqeYZjqZD5GE4v3/view?usp=sharing

```
gradle
                                                          R
   ==101583==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6100000000f3 at
   READ of size 1 at 0x6100000000f3 thread T0
2
     #0 0x6b0478 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0478)
3
4
     #1 0x6b99ca (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
     #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
5
     #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
6
     #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
7
     #5 0x7f173ed37c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
     #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
   0x6100000000f3 is located 0 bytes to the right of 179-byte region [0x610000000040,0x6
11
   allocated by thread T0 here:
12
     #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
     #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
14
15
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
   Shadow bytes around the buggy address:
17
    18
    19
    20
21
    0x0c207fff8000: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
22
   23
    24
    25
    26
    27
    28
   Shadow byte legend (one shadow byte represents 8 application bytes):
29
    Addressable:
30
                   00
```

```
Partially addressable: 01 02 03 04 05 06 07
31
      Heap left redzone:
32
                                 fa
33
      Freed heap region:
                                 fd
      Stack left redzone:
34
                                 f1
      Stack mid redzone:
35
                                 f2
      Stack right redzone:
                                f3
36
37
      Stack after return:
                                f5
38
      Stack use after scope:
                                f8
      Global redzone:
                                 f9
39
      Global init order:
                                 f6
40
      Poisoned by user:
                                 f7
41
      Container overflow:
                                 fc
42
      Array cookie:
43
                                 ac
      Intra object redzone:
44
                                 bb
45
      ASan internal:
                                 fe
      Left alloca redzone:
46
                                 ca
      Right alloca redzone:
47
                                 cb
48
      Shadow gap:
                                 СС
    ==101583==ABORTING
49
```

https://drive.google.com/file/d/1ekBLM7xmf0hegwcs0e2abmzlgKE4CfRJ/view?usp=sharing

```
R
gradle
    ==102014==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f3d201e5808 at
1
    READ of size 8 at 0x7f3d201e5808 thread T0
2
        #0 0x6c0473 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0473)
3
        #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
4
        #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
5
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6
        #4 0x7f3d24357c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
7
8
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
    0x7f3d201e5808 is located 8 bytes to the right of 1048576-byte region [0x7f3d200e5800
10
    allocated by thread T0 here:
11
12
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
        #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
13
        #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
14
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
15
        #4 0x7f3d24357c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
17
18
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
    Shadow bytes around the buggy address:
19
20
```

```
21
   22
   23
   24
   25
  =>0x0fe824034b00: fa[fa]fa fa fa
26
   27
   28
   29
30
   Shadow byte legend (one shadow byte represents 8 application bytes):
31
   Addressable:
32
33
   Partially addressable: 01 02 03 04 05 06 07
   Heap left redzone:
34
                 fa
   Freed heap region:
                 fd
35
   Stack left redzone:
36
                 f1
   Stack mid redzone:
                 f2
37
38
   Stack right redzone:
                 f3
                 f5
39
   Stack after return:
   Stack use after scope:
40
                 f8
   Global redzone:
                 f9
41
   Global init order:
                 f6
42
43
   Poisoned by user:
                 f7
44
   Container overflow:
                 fc
   Array cookie:
45
                 ac
   Intra object redzone:
46
                 bb
   ASan internal:
                 fe
47
   Left alloca redzone:
48
                 ca
   Right alloca redzone:
49
                 cb
50
   Shadow gap:
                 CC
  ==102014==ABORTING
51
```

https://drive.google.com/file/d/1z8NVVHQnZZeMwhZNPcNM-Jg64HNCU1qn/view?usp=sharing

```
gradle

1  ==102472==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fa28a7e5808 at
2  READ of size 8 at 0x7fa28a7e5808 thread T0

3  #0 0x6c0414 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0414)

4  #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)

5  #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)

6  #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)

7  #4 0x7fa28e8f7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

8  #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
```

```
9
10
   0x7fa28a7e5808 is located 8 bytes to the right of 1048576-byte region [0x7fa28a6e5800
   allocated by thread T0 here:
11
     #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
     #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
13
     #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
14
     #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
15
     #4 0x7fa28e8f7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
17
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
18
19
   Shadow bytes around the buggy address:
    20
21
    22
23
    24
   =>0x0ff4d14f4b00: fa[fa]fa fa fa
25
    26
27
    28
    29
    30
   Shadow byte legend (one shadow byte represents 8 application bytes):
31
32
    Addressable:
                    00
33
    Partially addressable: 01 02 03 04 05 06 07
    Heap left redzone:
                     fa
34
    Freed heap region:
                     fd
35
    Stack left redzone:
                     f1
36
37
    Stack mid redzone:
                     f2
    Stack right redzone:
                     f3
38
    Stack after return:
                     f5
39
    Stack use after scope:
40
                     f8
    Global redzone:
                     f9
41
    Global init order:
                     f6
42
43
    Poisoned by user:
                     f7
    Container overflow:
44
                     fc
    Array cookie:
45
                     ac
    Intra object redzone:
46
                     bb
    ASan internal:
47
                     fe
48
    Left alloca redzone:
                     ca
    Right alloca redzone:
49
                     cb
50
    Shadow gap:
                     CC
   ==102472==ABORTING
```

ASan internal:

fe

45

```
gradle
                                                               R
   ==102877==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000418 at
2
   READ of size 1 at 0x619000000418 thread T0
3
      #0 0x6b05ce (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05ce)
      #1 0x6b99ca (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
4
      #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
5
6
      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
7
      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
      #5 0x7fb14c4a8c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
   0x619000000418 is located 0 bytes to the right of 920-byte region [0x619000000080,0x6
11
12
   allocated by thread T0 here:
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
      #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
14
15
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
17
   Shadow bytes around the buggy address:
18
     19
     20
     21
     22
   =>0x0c327fff8080: 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa
23
     24
     25
     26
     27
     28
   Shadow byte legend (one shadow byte represents 8 application bytes):
29
30
     Addressable:
                     00
31
    Partially addressable: 01 02 03 04 05 06 07
32
    Heap left redzone:
                       fa
     Freed heap region:
                       fd
33
    Stack left redzone:
34
                       f1
35
    Stack mid redzone:
                       f2
36
    Stack right redzone:
                       f3
    Stack after return:
                       f5
37
    Stack use after scope:
                       f8
38
    Global redzone:
                       f9
39
    Global init order:
                       f6
40
    Poisoned by user:
                       f7
41
    Container overflow:
                       fc
42
43
    Array cookie:
                       ac
    Intra object redzone:
44
                       bb
```

```
46 Left alloca redzone: ca
47 Right alloca redzone: cb
48 Shadow gap: cc
49 ==102877==ABORTING
```

https://drive.google.com/file/d/1mzQOboXjXdBkuV4Bw8H577nkqXf4xWCu/view?usp=sharing

```
gradle
                                                             R
   ==103532==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f98ea3af808 at
1
2
   READ of size 8 at 0x7f98ea3af808 thread T0
3
      #0 0x6c0a32 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0a32)
      #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
4
5
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6
7
      #4 0x7f98f803ec86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
      #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
   0x7f98ea3af808 is located 8 bytes to the right of 1048576-byte region [0x7f98ea2af800
10
   allocated by thread T0 here:
11
12
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
      #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
13
      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
14
      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
15
      #4 0x7f98f803ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
17
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
18
19
   Shadow bytes around the buggy address:
20
    21
    22
    23
    24
   =>0x0ff39d46df00: fa[fa]fa fa fa
25
    26
27
    28
    29
    30
   Shadow byte legend (one shadow byte represents 8 application bytes):
31
    Addressable:
32
                     00
    Partially addressable: 01 02 03 04 05 06 07
33
    Heap left redzone:
                      fa
34
    Freed heap region:
35
                      fd
```

```
Stack left redzone:
                                 f1
36
                                 f2
37
       Stack mid redzone:
       Stack right redzone:
                                 f3
38
39
       Stack after return:
                                 f5
       Stack use after scope:
40
                                 f8
      Global redzone:
                                 f9
41
42
      Global init order:
                                 f6
43
       Poisoned by user:
                                 f7
44
      Container overflow:
                                 fc
      Array cookie:
45
                                 ac
       Intra object redzone:
46
                                 bb
      ASan internal:
                                 fe
47
       Left alloca redzone:
48
                                 ca
       Right alloca redzone:
49
                                 cb
50
       Shadow gap:
                                 CC
    ==103532==ABORTING
51
```

https://drive.google.com/file/d/1Vk\_ulbbK5FYfeczsEU6YBQv7t8rAjvdA/view?usp=sharing

```
gradle
                                                                                       R
    ==104121==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x617000007110 at
 1
    READ of size 4 at 0x617000007110 thread T0
 2
 3
        #0 0x6c0bc3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0bc3)
        #1 0x6baee8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
 4
        #2 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
 5
        #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
 6
 7
        #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #5 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
 8
                     (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
 9
10
11
    0x617000007110 is located 392 bytes to the right of 648-byte region [0x617000006d00,0
    freed by thread T0 here:
12
        #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aee
13
        #1 0x5add31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
14
        #2 0x540f73 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540f73)
15
        #3 0x6bc059 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bc059)
16
        #4 0x6baee8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
17
                     (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
        #5 0x6baee8
18
                     (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
19
        #6 0x527687
        #7 0x4fe3fe
                     (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
20
21
                     (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #8 0x4f5710
        #9 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
23
```

```
previously allocated by thread T0 here:
24
      #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aee
25
      #1 0x5add31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
26
      #2 0x540696 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540696)
27
      #3 0x6bda43 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bda43)
28
29
      #4 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
      #5 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
30
      #6 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
31
      #7 0x7f987337ac86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
32
33
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
34
   Shadow bytes around the buggy address:
35
    36
    37
    0x0c2e7fff8df0: fd fa fa
38
    39
    40
   =>0x0c2e7fff8e20: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa
41
    42
    43
    44
    45
    46
   Shadow byte legend (one shadow byte represents 8 application bytes):
47
    Addressable:
48
                     00
    Partially addressable: 01 02 03 04 05 06 07
49
    Heap left redzone:
                       fa
50
    Freed heap region:
51
                       fd
52
    Stack left redzone:
                       f1
    Stack mid redzone:
                       f2
53
    Stack right redzone:
                       f3
54
    Stack after return:
                       f5
55
    Stack use after scope:
56
                       f8
    Global redzone:
                       f9
57
    Global init order:
                       f6
58
    Poisoned by user:
59
                       f7
    Container overflow:
60
                       fc
    Array cookie:
61
                       ac
    Intra object redzone:
62
                       bb
63
    ASan internal:
                       fe
    Left alloca redzone:
64
                       ca
65
    Right alloca redzone:
                       cb
66
    Shadow gap:
                       СС
67
   ==104121==ABORTING
```

```
gradle
                                                                    R
  1
    ==104506==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60800000017a at
    WRITE of size 1 at 0x60800000017a thread T0
  2
        #0 0x6e412a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e412a)
  3
        #1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
  4
        #2 0x4fbe96 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe96)
  5
        #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
  6
  7
        #4 0x7f034a2f9c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
  8
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
  9
    0x60800000017a is located 0 bytes to the right of 90-byte region [0x608000000120,0x60
 10
    allocated by thread T0 here:
 11
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
 12
        #1 0x6e3519 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
 13
        #2 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
 14
 15
 16
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
    Shadow bytes around the buggy address:
 17
      18
      19
 20
      0x0c107fff8000: fa fa fa fd fd
 21
      0x0c107fff8010: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 01
 22
    =>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00 [02]
 23
      24
      25
      26
 27
      28
    Shadow byte legend (one shadow byte represents 8 application bytes):
 29
      Addressable:
 30
                        00
 31
      Partially addressable: 01 02 03 04 05 06 07
 32
      Heap left redzone:
                         fa
      Freed heap region:
 33
                         fd
      Stack left redzone:
                         f1
 34
      Stack mid redzone:
                         f2
 35
      Stack right redzone:
                         f3
 36
      Stack after return:
 37
                         f5
 38
      Stack use after scope:
                         f8
      Global redzone:
                         f9
 39
      Global init order:
                         f6
 40
      Poisoned by user:
 41
                         f7
      Container overflow:
                         fc
42
```

```
Array cookie:
43
                                 ac
44
      Intra object redzone:
                                 bb
45
      ASan internal:
                                 fe
      Left alloca redzone:
46
                                 ca
      Right alloca redzone:
47
                                 cb
48
       Shadow gap:
                                 CC
49
    ==104506==ABORTING
```

Addressable:

00

32

#### % sample file:

https://drive.google.com/file/d/10bToO-dwTYTBCiAxxkB4MSu7N8Vu6Nd0/view?usp=sharing

```
gradle
                                                                        R
   ==104877==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b000000db3 at
1
   WRITE of size 176 at 0x60b000000db3 thread T0
2
       #0 0x4adcdb in asan memset (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
3
       #1 0x5cd359 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5cd359)
4
       #2 0x4fea8d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fea8d)
5
       #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
7
       #4 0x7f604b90ec86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
       #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
   0x60b000000db3 is located 0 bytes to the right of 99-byte region [0x60b00000d50,0x60
10
   allocated by thread T0 here:
11
12
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
       #1 0x5cd14f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5cd14f)
13
       #2 0x4fea8d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fea8d)
14
       #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
15
       #4 0x7f604b90ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
16
17
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
18
   Shadow bytes around the buggy address:
19
     0x0c167fff8160: fa fa fa fa fa fa fa fd fd fd fd fd fd fd
20
     0x0c167fff8170: fd fd fd fd fa fa fa fa fa fa fa fa fa fa
21
     0x0c167fff8180: fd fa fa fa fa
22
     0x0c167fff8190: fa fa fa fd fd
23
24
     0x0c167fff81a0: fd fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00
   =>0x0c167fff81b0: 00 00 00 00 00 00[03]fa fa fa fa fa fa fa fa
25
     26
     27
     28
     29
     30
   Shadow byte legend (one shadow byte represents 8 application bytes):
31
```

```
Partially addressable: 01 02 03 04 05 06 07
33
      Heap left redzone:
34
                                 fa
35
      Freed heap region:
                                 fd
      Stack left redzone:
36
                                 f1
      Stack mid redzone:
37
                                 f2
      Stack right redzone:
                                f3
38
39
      Stack after return:
                                f5
40
      Stack use after scope:
                                f8
      Global redzone:
                                 f9
41
      Global init order:
                                 f6
42
43
      Poisoned by user:
                                 f7
      Container overflow:
                                 fc
44
      Array cookie:
45
                                 ac
      Intra object redzone:
46
                                 bb
      ASan internal:
47
                                 fe
      Left alloca redzone:
48
                                 ca
      Right alloca redzone:
49
                                 cb
50
      Shadow gap:
                                 СС
    ==104877==ABORTING
51
```

https://drive.google.com/file/d/1zwOiBamt4YehbcC4pAG6y0Ww9GOvKHBI/view?usp=sharing

```
R
gradle
    ==105392==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000030bc3 at
1
    WRITE of size 1 at 0x611000030bc3 thread T0
2
       #0 0x6e41a8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41a8)
3
       #1 0x5bea45 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)
4
       #2 0x4fbdd4 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbdd4)
5
       #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
6
       #4 0x7f34f993dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
7
8
       #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
    0x611000030bc3 is located 0 bytes to the right of 195-byte region [0x611000030b00,0x6
10
    allocated by thread T0 here:
11
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
       #1 0x6e3519 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
13
       #2 0x5bea45 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)
14
15
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
17
    Shadow bytes around the buggy address:
     18
     0x0c227fffe130: fa fa fa fa fa fa fa fd fd fd fd fd fd fd
19
     20
```

```
0x0c227fffe150: fd fd fd fd fa fa
21
    22
23
   =>0x0c227fffe170: 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa fa
24
    25
    26
    27
    28
   Shadow byte legend (one shadow byte represents 8 application bytes):
29
30
    Addressable:
                    00
31
    Partially addressable: 01 02 03 04 05 06 07
32
    Heap left redzone:
                     fa
33
    Freed heap region:
                     fd
    Stack left redzone:
                     f1
34
    Stack mid redzone:
                     f2
35
                     f3
36
    Stack right redzone:
    Stack after return:
                     f5
37
38
    Stack use after scope:
                     f8
    Global redzone:
                     f9
39
    Global init order:
                     f6
40
41
    Poisoned by user:
                     f7
    Container overflow:
                     fc
42
43
    Array cookie:
                     ac
    Intra object redzone:
44
                     bb
    ASan internal:
45
                     fe
    Left alloca redzone:
46
                     ca
    Right alloca redzone:
47
                     cb
    Shadow gap:
48
                     CC
49
   ==105392==ABORTING
```

https://drive.google.com/file/d/1WI9wJ79IXESIfL4ycvNzE-kN8\_AJIX9k/view?usp=sharing

#### % crash info

R gradle ==105898==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000000ec2 at 1 WRITE of size 1 at 0x616000000ec2 thread T0 2 #0 0x6e41b0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b0) 3 #1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f) 4 #2 0x4fbe60 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60) 5 #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932) 6 #4 0x7fd2baafcc86 in \_\_libc\_start\_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/ 7 #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549) 8 0x616000000ec2 is located 0 bytes to the right of 578-byte region [0x616000000c80,0x6 10

```
11
  allocated by thread T0 here:
     #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
12
13
     #1 0x6e3519 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
     #2 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
14
15
  SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
17
  Shadow bytes around the buggy address:
    18
    19
20
    21
22
    23
  =>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa
24
    25
    26
    27
    28
  Shadow byte legend (one shadow byte represents 8 application bytes):
29
    Addressable:
                  00
30
    Partially addressable: 01 02 03 04 05 06 07
31
    Heap left redzone:
32
                    fa
    Freed heap region:
                    fd
33
    Stack left redzone:
34
                    f1
35
    Stack mid redzone:
                    f2
    Stack right redzone:
                    f3
36
    Stack after return:
37
                    f5
    Stack use after scope:
                    f8
38
39
    Global redzone:
                    f9
    Global init order:
                    f6
40
    Poisoned by user:
                    f7
41
    Container overflow:
42
                    fc
    Array cookie:
43
                    ac
    Intra object redzone:
44
                    bb
    ASan internal:
45
                    fe
    Left alloca redzone:
46
                    ca
    Right alloca redzone:
47
                    cb
    Shadow gap:
48
                    CC
  ==105898==ABORTING
49
```

https://drive.google.com/file/d/10HnRlC6e-FAFZnKpQjZengXfKKvlzj-Q/view?usp=sharing

% crash info

→ gradle



```
==106312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000ec2 at
 1
    WRITE of size 1 at 0x616000000ec2 thread T0
 2
 3
       #0 0x6e41b8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b8)
 4
       #1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
       #2 0x4fbe60 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60)
 5
       #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
 6
 7
       #4 0x7f5a9e97cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
       #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
 8
 9
    0x616000000ec2 is located 0 bytes to the right of 578-byte region [0x616000000c80,0x6
 10
    allocated by thread T0 here:
 11
       #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
 12
       #1 0x6e3519 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
 13
       #2 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
 14
 15
    SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
 16
    Shadow bytes around the buggy address:
 17
 18
      19
     20
 21
     22
     =>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa
 23
     24
     25
     26
     27
      28
 29
    Shadow byte legend (one shadow byte represents 8 application bytes):
     Addressable:
 30
                      00
     Partially addressable: 01 02 03 04 05 06 07
 31
     Heap left redzone:
 32
                        fa
     Freed heap region:
                        fd
 33
     Stack left redzone:
                        f1
 34
     Stack mid redzone:
 35
                        f2
     Stack right redzone:
 36
                        f3
     Stack after return:
 37
                        f5
     Stack use after scope:
 38
                        f8
     Global redzone:
 39
                        f9
 40
     Global init order:
                        f6
     Poisoned by user:
 41
                        f7
     Container overflow:
                        fc
 42
     Array cookie:
 43
                        ac
     Intra object redzone:
 44
                        bb
     ASan internal:
                        fe
 45
     Left alloca redzone:
 46
                        ca
     Right alloca redzone:
 47
                        cb
$ 48
     Shadow gap:
                        CC
    ==106312==ABORTING
 49
```

https://drive.google.com/file/d/1lrGT3ll8CXwJXYvPj57JUDs\_FAO2k\_MT/view?usp=sharing

```
gradle
                                                                    R
   ==107115==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60e00000037b at
2
   WRITE of size 1 at 0x60e00000037b thread T0
3
      #0 0x6e420d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e420d)
4
      #1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
5
      #2 0x4fbe96 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe96)
6
      #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
7
      #4 0x7f3dd47a6c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
      #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
   0x60e00000037b is located 0 bytes to the right of 155-byte region [0x60e0000002e0,0x6
11
   allocated by thread T0 here:
12
      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
      #1 0x6e3519 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
14
      #2 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
15
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
16
   Shadow bytes around the buggy address:
17
     0x0c1c7fff8010: fd fa fa fa
18
19
     0x0c1c7fff8020: fa fa fa fd fd
     0x0c1c7fff8030: fd fd fd fd fd fd fd fa fa fa fa fa fa fa
20
21
     22
     0x0c1c7fff8050: 00 00 00 02 fa fa fa fa fa fa fa fa o0 00 00 00
23
   24
25
     26
     27
28
     29
   Shadow byte legend (one shadow byte represents 8 application bytes):
30
     Addressable:
                       00
     Partially addressable: 01 02 03 04 05 06 07
31
32
     Heap left redzone:
                         fa
33
     Freed heap region:
                         fd
34
     Stack left redzone:
                         f1
35
     Stack mid redzone:
                        f2
36
     Stack right redzone:
                        f3
37
     Stack after return:
                         f5
     Stack use after scope:
38
                         f8
     Global redzone:
                         f9
```

```
Global init order:
40
                                 f6
                                 f7
41
      Poisoned by user:
      Container overflow:
                                 fc
42
43
      Array cookie:
                                 ac
      Intra object redzone:
44
                                 bb
45
      ASan internal:
                                 fe
46
      Left alloca redzone:
                                 ca
47
      Right alloca redzone:
                                 cb
       Shadow gap:
48
                                 CC
    ==107115==ABORTING
49
```

https://drive.google.com/file/d/1JbvorHMKI3foPIGEozLWKhWkLFX3-yUQ/view?usp=sharing

```
gradle
                                                          R
   ==107517==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b0000000660 at
1
   READ of size 1 at 0x61b000000660 thread T0
2
3
     #0 0x65fc97 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65fc97)
     #1 0x4fe89d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
4
     #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
5
     #3 0x7fe052acac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
6
7
     #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
9
   0x61b000000660 is located 0 bytes to the right of 1504-byte region [0x61b000000080,0x
   allocated by thread T0 here:
10
     #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
11
12
     #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
     #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
13
14
     #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
     #4 0x7fe052acac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
15
16
   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17
   Shadow bytes around the buggy address:
18
    19
20
    21
    22
    23
    24
   =>0x0c367fff80c0: 00 00 00 00 00 00 00 00 00 00 00 00 [fa]fa fa fa
25
    26
    27
    28
    29
```

```
Shadow byte legend (one shadow byte represents 8 application bytes):
30
       Addressable:
31
                               00
32
      Partially addressable: 01 02 03 04 05 06 07
      Heap left redzone:
33
                                 fa
      Freed heap region:
34
                                 fd
35
      Stack left redzone:
                                 f1
      Stack mid redzone:
36
                                 f2
37
      Stack right redzone:
                                 f3
      Stack after return:
                                 f5
38
39
      Stack use after scope:
                                 f8
40
      Global redzone:
                                 f9
      Global init order:
                                 f6
41
42
      Poisoned by user:
                                 f7
      Container overflow:
                                 fc
43
      Array cookie:
44
                                 ac
      Intra object redzone:
45
                                 bb
      ASan internal:
                                 fe
46
47
      Left alloca redzone:
                                 ca
      Right alloca redzone:
48
                                 cb
49
      Shadow gap:
                                 CC
    ==107517==ABORTING
50
```

https://drive.google.com/file/d/19NCya7nuaUHr5XMLNyDcfD-bKCygnFL-/view?usp=sharing

```
gradle
                                                                                       R
    ==108318==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000005cb at
    READ of size 1 at 0x6120000005cb thread T0
 2
        #0 0x6b544e (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b544e)
 3
        #1 0x6b6bf3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6bf3)
 4
        #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
 5
 6
        #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
 7
        #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #5 0x7f0873f24c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
 8
        #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
 9
10
    0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
11
    allocated by thread T0 here:
12
        #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13
        #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
14
        #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
15
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
16
        #4 0x7f0873f24c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
18
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
19
  Shadow bytes around the buggy address:
20
21
    0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
    22
23
    0x0c247fff8090: fa fa fa fa fa fa fa fa oo 00 00 00 00 00 00 00
24
    25
  =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
26
    27
28
    29
    30
    31
32
  Shadow byte legend (one shadow byte represents 8 application bytes):
    Addressable:
33
                   00
34
    Partially addressable: 01 02 03 04 05 06 07
35
    Heap left redzone:
                    fa
    Freed heap region:
36
                    fd
    Stack left redzone:
37
                    f1
    Stack mid redzone:
                    f2
38
    Stack right redzone:
                    f3
39
    Stack after return:
                    f5
40
    Stack use after scope: f8
41
    Global redzone:
42
                    f9
    Global init order:
                    f6
43
    Poisoned by user:
                    f7
44
    Container overflow:
45
                    fc
    Array cookie:
46
                    ac
47
    Intra object redzone:
                    bb
    ASan internal:
                    fe
48
    Left alloca redzone:
49
                    ca
    Right alloca redzone:
50
                    cb
    Shadow gap:
51
                    CC
52
  ==108318==ABORTING
```

## 8

# % catalogue 2: Vulnerability type – global heap buffer overflow

% sample file:

https://drive.google.com/file/d/1q4YevANr8ZSFnWHb1RLY34u3Blil7K3J/view?usp=sharing





```
==15097==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000075fb88 at
1
   READ of size 4 at 0x00000075fb88 thread T0
2
3
      #0 0x718693 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x718693)
4
      #1 0x6f835d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6f835d)
      #2 0x4f5ad3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5ad3)
5
      #3 0x7f69023d2c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
6
7
      #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
8
   0x00000075fb88 is located 56 bytes to the left of global variable 'cDigitsLut' define
9
   0x00000075fb88 is located 0 bytes to the right of global variable 'kPow10' defined in
10
   SUMMARY: AddressSanitizer: global-buffer-overflow (/home/bupt/Desktop/otfcc/bin/relea
11
12
   Shadow bytes around the buggy address:
13
     14
     0x0000800e3f30: 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9
15
     16
17
     0x0000800e3f60: 00 00 00 00 00 f9 f9 f9 f9 f9 00 00 00 00
   =>0x0000800e3f70: 00[f9]f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00
18
     19
     0x0000800e3f90: 00 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
20
     21
     22
     23
24
   Shadow byte legend (one shadow byte represents 8 application bytes):
25
     Addressable:
                       00
     Partially addressable: 01 02 03 04 05 06 07
26
     Heap left redzone:
27
                         fa
     Freed heap region:
                        fd
28
29
     Stack left redzone:
                        f1
     Stack mid redzone:
                        f2
30
     Stack right redzone:
                        f3
31
     Stack after return:
                        f5
32
                        f8
     Stack use after scope:
33
     Global redzone:
                        f9
34
     Global init order:
35
                        f6
     Poisoned by user:
36
                         f7
     Container overflow:
                        fc
37
     Array cookie:
38
                         ac
     Intra object redzone:
39
                        bb
40
     ASan internal:
                         fe
     Left alloca redzone:
41
                         ca
42
     Right alloca redzone:
                         cb
43
     Shadow gap:
                         CC
44
   ==15097==ABORTING
```

----}

## % catalogue 3: Vulnerability type – SEGV

#### % sample file:

https://drive.google.com/file/d/1-sFx\_eHoSXa79pye6Cdv2i2zvAfHwsGI/view?usp=sharing

% crash info

```
gradle
                                                                                   AddressSanitizer: DEADLYSIGNAL
 1
 2
    ______
    ==6233==ERROR: AddressSanitizer: SEGV on unknown address 0x6120002ad5dd (pc 0x7fbef83
    ==6233==The signal is caused by a READ memory access.
 4
 5
    ==6233==WARNING: failed to fork (errno 12)
    ==6233==WARNING: failed to fork (errno 12)
 6
 7
    ==6233==WARNING: failed to fork (errno 12)
    ==6233==WARNING: failed to fork (errno 12)
 8
    ==6233==WARNING: failed to fork (errno 12)
 9
    ==6233==WARNING: Failed to use and restart external symbolizer!
10
        #0 0x7fbef8354384 (/lib/x86 64-linux-gnu/libc.so.6+0xbb384)
11
        #1 0x4ad6eb (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4ad6eb)
12
13
        #2 0x6b53ed (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
        #3 0x6b6d86 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6d86)
14
        #4 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
15
        #5 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
16
        #6 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
17
        #7 0x7fbef82bac86 (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
18
        #8 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
19
20
    AddressSanitizer can not provide additional info.
21
    SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
22
    ==6233==ABORTING
23
```

## % sample file:

https://drive.google.com/file/d/1xdw71uUMvagCwPort6Uh6uktU67Jgrex/view?usp=sharing

```
#1 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
#2 0x7fada3943c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
#3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0

==9104==ABORTING
```

https://drive.google.com/file/d/1UuJo7ifneTeY5j\_ZILPG4y8XgAIUm2eE/view?usp=sharing

% crash info

```
routeros
                                                                                  AddressSanitizer: DEADLYSIGNAL
2
    ______
    ==10580==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x0000000
3
    ==10580==The signal is caused by a READ memory access.
4
    ==10580==Hint: address points to the zero page.
5
    ==10580==WARNING: failed to fork (errno 12)
6
7
    ==10580==WARNING: failed to fork (errno 12)
    ==10580==WARNING: failed to fork (errno 12)
9
    ==10580==WARNING: failed to fork (errno 12)
    ==10580==WARNING: failed to fork (errno 12)
10
    ==10580==WARNING: Failed to use and restart external symbolizer!
11
        #0 0x4fe9a7 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe9a7)
12
        #1 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
13
        #2 0x7f16ea646c86 (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
14
        #3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
15
16
    AddressSanitizer can not provide additional info.
17
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
18
    ==10580==ABORTING
19
```

#### % sample file:

https://drive.google.com/file/d/10rlHDs0V6s2DrbjcYwWAoF2kd2\_fao7M/view?usp=sharing

```
4
    ==128856==The signal is caused by a READ memory access.
        #0 0x7fdeb5ff1384 /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86 64/multia
 5
        #1 0x4ad6eb in __asan_memcpy (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
 6
 7
        #2 0x6b53ed (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
        #3 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
 8
        #4 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
 9
10
        #5 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
        #6 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
11
        #7 0x7fdeb5f57c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
12
        #8 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
13
14
    AddressSanitizer can not provide additional info.
15
    SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86
16
    ==128856==ABORTING
17
```

https://drive.google.com/file/d/1tkNyCltred6mhLx2Um1ZsyAthH55DClW/view?usp=sharing

## % crash info

```
gradle
                                                                                  R
    AddressSanitizer:DEADLYSIGNAL
1
2
    ______
3
    ==130785==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000004 (pc 0x00000
    ==130785==The signal is caused by a READ memory access.
4
5
    ==130785==Hint: address points to the zero page.
    ==130785==WARNING: failed to fork (errno 12)
    ==130785==WARNING: failed to fork (errno 12)
7
    ==130785==WARNING: failed to fork (errno 12)
8
9
    ==130785==WARNING: failed to fork (errno 12)
    ==130785==WARNING: failed to fork (errno 12)
10
    ==130785==WARNING: Failed to use and restart external symbolizer!
11
        #0 0x5266a8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5266a8)
12
        #1 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
13
        #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
14
        #3 0x7f952a4e0c86 (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
15
        #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
16
17
    AddressSanitizer can not provide additional info.
18
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
19
    ==130785==ABORTING
20
```

#### % sample file:

```
gradle
                                                                                 AddressSanitizer: DEADLYSIGNAL
2
    ______
3
    ==1197==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000004cc (pc 0x00000006
    ==1197==The signal is caused by a READ memory access.
4
5
    ==1197==Hint: address points to the zero page.
6
        #0 0x6badae (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6badae)
7
       #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
       #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
8
9
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
10
        #4 0x7f62e925ec86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12
    AddressSanitizer can not provide additional info.
13
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
14
    ==1197==ABORTING
15
```

https://drive.google.com/file/d/1PXIJGUbUZxReuOTEuF8Pvny5hjNtXzJI/view?usp=sharing

#### % crash info

```
gradle
                                                                                R
    AddressSanitizer: DEADLYSIGNAL
1
    _____
2
3
    ==2966==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000036 (pc 0x00000004
    ==2966==The signal is caused by a READ memory access.
4
    ==2966==Hint: address points to the zero page.
5
        #0 0x4fbbb6 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbbb6)
6
       #1 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
7
8
        #2 0x7f3e141cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
        #3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
    AddressSanitizer can not provide additional info.
11
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
12
    ==2966==ABORTING
13
```

#### % sample file :

https://drive.google.com/file/d/18tbZsfm\_CgaAoB5L\_22EFCF\_DWTYrAVg/view?usp=sharing



gradle

```
AddressSanitizer: DEADLYSIGNAL
1
2
    ______
    ==3991==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000006 (pc 0x00000004
3
    ==3991==The signal is caused by a READ memory access.
4
    ==3991==Hint: address points to the zero page.
5
        #0 0x4fe954 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe954)
6
7
        #1 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #2 0x7fee2bb48c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
8
        #3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10
11
    AddressSanitizer can not provide additional info.
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
12
    ==3991==ABORTING
13
```

## % sample file:

https://drive.google.com/file/d/1h41bo6TRBhd16kADaBcJpSWiW76WtDsM/view?usp=sharing

#### % crash info

```
gradle
                                                                                 R
    AddressSanitizer: DEADLYSIGNAL
1
2
    _____
    ==8370==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000704 (pc 0x00000006
3
    ==8370==The signal is caused by a READ memory access.
4
    ==8370==Hint: address points to the zero page.
5
        #0 0x6babea (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6babea)
6
7
        #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
        #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
8
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
9
        #4 0x7f8358612c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12
    AddressSanitizer can not provide additional info.
13
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
14
15
    ==8370==ABORTING
```

#### % sample file:

https://drive.google.com/file/d/1VBUoaxBplTvecwySIm\_tuvRIsnIdIGAF/view?usp=sharing





```
AddressSanitizer: DEADLYSIGNAL
1
2
    _____
3
    ==9840==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x00000006
    ==9840==The signal is caused by a READ memory access.
4
5
    ==9840==Hint: address points to the zero page.
        #0 0x6b6a8f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6a8f)
6
7
       #1 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
       #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
8
9
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #4 0x7f4071149c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12
    AddressSanitizer can not provide additional info.
13
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
14
15
    ==9840==ABORTING
```

https://drive.google.com/file/d/1QYTVBayBwZvLdp4VNklxB696V8jmnxU6/view?usp=sharing

#### % crash info

```
gradle
                                                                                  R
    AddressSanitizer: DEADLYSIGNAL
1
2
    _____
3
    ==1585==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x000000703969 bp 0x7ffd
    ==1585==The signal is caused by a READ memory access.
4
5
    ==1585==Hint: this fault was caused by a dereference of a high value address (see reg
6
        #0 0x703969 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x703969)
        #1 0x65be5b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65be5b)
7
        #2 0x4fe2f1 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe2f1)
8
9
        #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
        #4 0x7f72f8d40c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10
        #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12
    AddressSanitizer can not provide additional info.
13
    SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
14
    ==1585==ABORTING
15
```

#### % sample file:

https://drive.google.com/file/d/1v5-qJeZpmw7\_txAnhl8ew82NW2BCdLFH/view?usp=sharing





```
grad<u>le_____</u>
  2
      ==1985==ERROR: AddressSanitizer: SEGV on unknown address 0x61b000010076 (pc 0x00000006
  3
      ==1985==The signal is caused by a READ memory access.
  4
         #0 0x65f724 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65f724)
  5
         #1 0x4fe89d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
  6
         #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
  7
         #3 0x7f4881d74c86 in libc start main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
         #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
  8
  9
 10
     AddressSanitizer can not provide additional info.
     SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
 11
     ==1985==ABORTING
 12
% received CVE id
% CVE-2022-33047
% Vulnerability type
use-after-free
% sample file :
https://drive.google.com/file/d/1g3MQajVLZAaZMRfIQHSLT6XRw-B4Dmz8/view?usp=sharing
% command to reproduce:
 shell
                                                                                       R
     ./otfccbuild -O3 -q --force-cid [sample file] -o /dev/null
% crash info
 shell
                                                                                       R
     ==49487==ERROR: AddressSanitizer: heap-use-after-free on address 0x603000000011 at pc
  1
     READ of size 1 at 0x603000000011 thread T0
  3
         #0 0x44cfbe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x44cfbe)
  4
         #1 0x44e7dd in vsnprintf (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4
         #2 0x72a75e (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x72a75e)
  5
         #3 0x72afc2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x72afc2)
  6
         #4 0x4f65ac (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4f65ac)
  7
         #5 0x7f6e50b86c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
  8
         #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x41c549)
  9
 10
     0x60300000011 is located 1 bytes inside of 20-byte region [0x60300000010,0x60300000
 11
```

freed by thread T0 here:

**1**2

```
13
      #0 0x4ae7d2 in free (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4ae7d2
14
      #1 0x4f5cf4 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4f5cf4)
      #2 0x7f6e50b86c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
15
16
17
   previously allocated by thread T0 here:
18
      #0 0x4aeb10 in malloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4aeb
19
      #1 0x724f05 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x724f05)
20
   SUMMARY: AddressSanitizer: heap-use-after-free (/home/bupt/Desktop/otfcc/bin/release-
21
   Shadow bytes around the buggy address:
22
23
     24
     25
     26
     27
   =>0x0c067fff8000: fa fa[fd]fd fd fa fa fa fd fd fd fa fa fa fd
28
     0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fd fd fd fa fa fa
29
     0x0c067fff8020: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd
30
31
     0x0c067fff8030: fa fa fd fd fa fa fa fd fd fd fa fa fa fa
     32
     33
   Shadow byte legend (one shadow byte represents 8 application bytes):
34
35
     Addressable:
                      00
     Partially addressable: 01 02 03 04 05 06 07
36
37
    Heap left redzone:
                        fa
    Freed heap region:
                        fd
38
    Stack left redzone:
                        f1
39
    Stack mid redzone:
                        f2
40
    Stack right redzone:
                        f3
41
    Stack after return:
42
                        f5
    Stack use after scope:
43
                        f8
    Global redzone:
                        f9
44
    Global init order:
45
                        f6
    Poisoned by user:
46
                        f7
    Container overflow:
47
                        fc
    Array cookie:
48
                        ac
49
    Intra object redzone:
                        bb
    ASan internal:
                        fe
50
    Left alloca redzone:
51
                        ca
     Right alloca redzone:
52
                        cb
     Shadow gap:
53
                        CC
54
   ==49487==ABORTING
```

- - - 8°

Author: Victory+

**Link:** https://cvjark.github.io/2022/07/06/CVE-2022-33047/

Copyright Notice: All articles in this blog are licensed under CC BY-NC-SA 4.0 unless stating additionally.





Local search

Search for Posts



Powered by <u>hexo-generator-search</u>

×

