

otfcc's issue Reference

 2022-07-06 |  bug disclosure |  0 Comments

Word count: 20k | Reading time: 125 min

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 :

 <https://drive.google.com/file/d/1m8K86hpdDFDC2KcbD2QQ3yAD2zpBrA2f/view?usp=sharing>

gradle



```

1  ==100398==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
2  READ of size 4294967295 at 0x61200000044b thread T0
3      #0 0x4adb11 in __asan_memcpy (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
4      #1 0x6b53ed (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
5      #2 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
6      #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
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 0x7f6a7f4b6c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10     #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12 0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
13 allocated by thread T0 here:
14     #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8
15     #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
16     #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 0x7f6a7f4b6c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
19
20 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
21 Shadow bytes around the buggy address:
22     0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
23     0x0c247fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24     0x0c247fff8050: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
25     0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
26     0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 =>0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
28     0x0c247fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29     0x0c247fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30     0x0c247fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31     0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32     0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33 Shadow byte legend (one shadow byte represents 8 application bytes):
34 Addressable:                00
35 Partially addressable: 01 02 03 04 05 06 07
36 Heap left redzone:          fa
37 Freed heap region:           fd
38 Stack left redzone:          f1
39 Stack mid redzone:           f2
40 Stack right redzone:         f3
41 Stack after return:          f5
42 Stack use after scope:       f8
43 Global redzone:              f9
44 Global init order:           f6
45 Poisoned by user:           f7

```

```

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

```

 sample file :

https://drive.google.com/file/d/1BZ_T5C1cPfYgyueIBJ8vu45zZcSNhJAt/view?usp=sharing

 crash info

gradle



```

1  =====
2  ==111746==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
3  READ of size 1 at 0x61200000044b thread T0
4      #0 0x6b558f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b558f)
5      #1 0x6b6bf3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6bf3)
6      #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
7      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
8      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
9      #5 0x7ff49f52ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10     #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12 0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
13 allocated by thread T0 here:
14     #0 0x4aecdb in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdb
15     #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
16     #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 0x7ff49f52ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
19
20 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
21 Shadow bytes around the buggy address:
22   0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
23   0x0c247fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24   0x0c247fff8050: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
25   0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
26   0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 =>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
28   0x0c247fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c247fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c247fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```



```

32  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33  Shadow byte legend (one shadow byte represents 8 application bytes):
34  Addressable:          00
35  Partially addressable: 01 02 03 04 05 06 07
36  Heap left redzone:    fa
37  Freed heap region:    fd
38  Stack left redzone:    f1
39  Stack mid redzone:     f2
40  Stack right redzone:   f3
41  Stack after return:    f5
42  Stack use after scope: f8
43  Global redzone:        f9
44  Global init order:     f6
45  Poisoned by user:      f7
46  Container overflow:    fc
47  Array cookie:          ac
48  Intra object redzone:  bb
49  ASan internal:         fe
50  Left alloca redzone:   ca
51  Right alloca redzone:  cb
52  Shadow gap:            cc
53  ==111746==ABORTING

```

 sample file :

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

 crash info

gradle



```

1  =====
2  ==117024==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000832 at
3  READ of size 1 at 0x616000000832 thread T0
4    #0 0x6e7e3d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e7e3d)
5    #1 0x5eb58a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb58a)
6    #2 0x4fe227 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
7    #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
8    #4 0x7fcd6ac0dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9    #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11  0x616000000832 is located 680 bytes to the right of 522-byte region [0x616000000380,0
12  allocated by thread T0 here:
13    #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8
14    #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
15    #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
16    #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
17    #4 0x7fcd6ac0dc86 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   0x0c2c7fff80b0: 00 02 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
22   0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
23   0x0c2c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
24   0x0c2c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c2c7fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26 =>0x0c2c7fff8100: fa fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa
27   0x0c2c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c2c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c2c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c2c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c2c7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 Shadow byte legend (one shadow byte represents 8 application bytes):
33   Addressable:           00
34   Partially addressable: 01 02 03 04 05 06 07
35   Heap left redzone:      fa
36   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:  f8
42   Global redzone:         f9
43   Global init order:      f6
44   Poisoned by user:       f7
45   Container overflow:     fc
46   Array cookie:           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 ==117024==ABORTING

```

 sample file :

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

 crash info

gradle



```

1 ==106716==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000837 at
2 READ of size 1 at 0x616000000837 thread T0
3   #0 0x6e1fc8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e1fc8)
➔ 4   #1 0x5eb5ec (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb5ec)

```

```

5      #2 0x4fe227 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
6      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
7      #4 0x7fdfdc8c8c86 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 0x616000000837 is located 685 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      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
15      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
16      #4 0x7fdfdc8c8c86 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 Shadow bytes around the buggy address:
20      0x0c2c7fff80b0: 00 02 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
21      0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
22      0x0c2c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
23      0x0c2c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
24      0x0c2c7fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25 =>0x0c2c7fff8100: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa fa
26      0x0c2c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27      0x0c2c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28      0x0c2c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29      0x0c2c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30      0x0c2c7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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:          fa
35 Freed heap region:          fd
36 Stack left redzone:         f1
37 Stack mid redzone:          f2
38 Stack right redzone:        f3
39 Stack after return:         f5
40 Stack use after scope:      f8
41 Global redzone:             f9
42 Global init order:          f6
43 Poisoned by user:           f7
44 Container overflow:         fc
45 Array cookie:               ac
46 Intra object redzone:       bb
47 ASan internal:              fe
48 Left alloca redzone:        ca
49 Right alloca redzone:       cb
50 Shadow gap:                 cc
51 ==106716==ABORTING

```



🔗 sample file :

https://drive.google.com/file/d/1UQx_BSWEGqa18psFBjhkusjFvDA0ER_Z/view?usp=sharing

🔗 crash info

gradle



```
1  =====
2  ==107908==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000005cb at
3  READ of size 1 at 0x612000005cb 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)
6      #2 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
7      #3 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
8      #4 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
9      #5 0x7fc74767cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10     #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12 0x612000005cb is located 0 bytes to the right of 267-byte region [0x612000004c0,0x6
13 allocated by thread T0 here:
14     #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8)
15     #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
16     #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 0x7fc74767cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
19
20 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
21 Shadow bytes around the buggy address:
22   0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
23   0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24   0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa
25   0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
26   0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
28   0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32   0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33 Shadow byte legend (one shadow byte represents 8 application bytes):
34   Addressable:          00
35   Partially addressable: 01 02 03 04 05 06 07
36   Heap left redzone:    fa
37   Freed heap region:    fd
38   Stack left redzone:   f1
39   Stack mid redzone:    f2
40   Stack right redzone:  f3
41   Stack after return:   f5
```

```

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

```

 sample file :

https://drive.google.com/file/d/1CdFTd5Emf_jDRLv1z64W5Rm3O1Q1JTyQ/view?usp=sharing

 crash info

gradle



```

1  ==108759==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000616 at
2  READ of size 1 at 0x612000000616 thread T0
3      #0 0x6b064d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b064d)
4      #1 0x6b256a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
5      #2 0x6b74c0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
6      #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
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 0x7f93b614bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10     #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12 0x612000000616 is located 75 bytes to the right of 267-byte region [0x6120000004c0,0x
13  allocated by thread T0 here:
14     #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc)
15     #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
16     #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 0x7f93b614bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
19
20 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
21 Shadow bytes around the buggy address:
22   0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
24   0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
25   0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26   0x0c247fff80b0: 00 00 00 00 00 00 00 00 00 03 fa fa fa fa fa fa
27   =>0x0c247fff80c0: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa

```



```

28 0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30 0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31 0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 0x0c247fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33 Shadow byte legend (one shadow byte represents 8 application bytes):
34 Addressable:           00
35 Partially addressable: 01 02 03 04 05 06 07
36 Heap left redzone:      fa
37 Freed heap region:      fd
38 Stack left redzone:     f1
39 Stack mid redzone:      f2
40 Stack right redzone:    f3
41 Stack after return:     f5
42 Stack use after scope:  f8
43 Global redzone:         f9
44 Global init order:      f6
45 Poisoned by user:       f7
46 Container overflow:     fc
47 Array cookie:           ac
48 Intra object redzone:   bb
49 ASan internal:          fe
50 Left alloca redzone:    ca
51 Right alloca redzone:   cb
52 Shadow gap:             cc
53 ==108759==ABORTING

```

 sample file :

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

 crash info

gradle



```

1 ==109163==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000008bd at
2 READ of size 1 at 0x6120000008bd thread T0
3 #0 0x6adb1e (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6adb1e)
4 #1 0x6b71de (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b71de)
5 #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 0x7f199d870c86 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 0x6120000008bd is located 754 bytes to the right of 267-byte region [0x6120000004c0,0
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      #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 0x7f199d870c86 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   0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
22   0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
23   0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
24   0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26 =>0x0c247fff8110: fa fa fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa
27   0x0c247fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c247fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c247fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c247fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c247fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 Shadow byte legend (one shadow byte represents 8 application bytes):
33   Addressable:           00
34   Partially addressable: 01 02 03 04 05 06 07
35   Heap left redzone:      fa
36   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:  f8
42   Global redzone:         f9
43   Global init order:      f6
44   Poisoned by user:       f7
45   Container overflow:     fc
46   Array cookie:           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 ==109163==ABORTING

```

🔗 sample file :

https://drive.google.com/file/d/15zqWcqkig0fr36a7wOqurSltd1rq9n0_/view?usp=sharing

🔗 crash info

➔ gradle



```

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)
4      #1 0x5eb5ec (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb5ec)
5      #2 0x4fe227 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
6      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
7      #4 0x7f2da0c05c86 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 Address 0x6160000078a6 is a wild pointer.
11 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
12 Shadow bytes around the buggy address:
13   0x0c2c7fff8ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
14   0x0c2c7fff8ed0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
15   0x0c2c7fff8ee0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
16   0x0c2c7fff8ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
17   0x0c2c7fff8f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
18 =>0x0c2c7fff8f10: fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa
19   0x0c2c7fff8f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
20   0x0c2c7fff8f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
21   0x0c2c7fff8f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
22   0x0c2c7fff8f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
23   0x0c2c7fff8f60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
24 Shadow byte legend (one shadow byte represents 8 application bytes):
25   Addressable:                00
26   Partially addressable: 01 02 03 04 05 06 07
27   Heap left redzone:          fa
28   Freed heap region:           fd
29   Stack left redzone:         f1
30   Stack mid redzone:          f2
31   Stack right redzone:        f3
32   Stack after return:         f5
33   Stack use after scope:      f8
34   Global redzone:             f9
35   Global init order:          f6
36   Poisoned by user:           f7
37   Container overflow:         fc
38   Array cookie:               ac
39   Intra object redzone:       bb
40   ASan internal:              fe
41   Left alloca redzone:        ca
42   Right alloca redzone:       cb
43   Shadow gap:                 cc
44  ==109553==ABORTING

```

 sample file :



<https://drive.google.com/file/d/1RAiaUZVDjKj2yD52KOD13u6b9mdkN8WC/view?usp=sharing>

gradle



```

1  ==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)
4      #1 0x4fe1e2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe1e2)
5      #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
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:
11      #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc
12      #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
14      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
15      #4 0x7f502f9c0c86 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   0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c047fff8000: fa fa 00 00 fa fa 00 03 fa fa fd fa fa fa 00 03
22   0x0c047fff8010: fa fa fd fa fa fa 00 00 fa fa fd fa fa fa fd fa
23   0x0c047fff8020: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
24   =>0x0c047fff8030: fa fa 04 fa fa fa 00 fa fa fa[06]fa fa fa fd fa
25   0x0c047fff8040: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
26   0x0c047fff8050: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
27   0x0c047fff8060: fa fa fd fa fa fa 00 00 fa fa fa fa fa fa fa fa
28   0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30 Shadow byte legend (one shadow byte represents 8 application bytes):
31   Addressable:           00
32   Partially addressable: 01 02 03 04 05 06 07
33   Heap left redzone:      fa
34   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:  f8
40   Global redzone:         f9
41   Global init order:      f6
42   Poisoned by user:       f7
43   Container overflow:     fc
44   Array cookie:           ac
45   Intra object redzone:   bb

```

```

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

```

🔗 sample file :

<https://drive.google.com/file/d/1Gtp0aHRoRq5pDa73jXMcBZllsu2dCs7B/view?usp=sharing>

🔗 crash info

gradle



```

1  ==110431==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
2  READ of size 1 at 0x61200000044b thread T0
3      #0 0x6b559f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b559f)
4      #1 0x6b6d86 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6d86)
5      #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 0x7f17f472ec86 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      #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 0x7f17f472ec86 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   0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
22   0x0c247fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0c247fff8050: 00 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   0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26 =>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
27   0x0c247fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c247fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c247fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 Shadow byte legend (one shadow byte represents 8 application bytes):
33 Addressable:           00
34 Partially addressable: 01 02 03 04 05 06 07

```

```

35 Heap left redzone:      fa
36 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:  f8
42 Global redzone:         f9
43 Global init order:      f6
44 Poisoned by user:       f7
45 Container overflow:     fc
46 Array cookie:           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 ==110431==ABORTING

```

 sample file :

https://drive.google.com/file/d/1COw6yyyp8w99fEVhoeBz9mBw4h0_aZi_n/view?usp=sharing

 crash info

gradle



```

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

```

```

22 0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
23 0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24 0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
25 0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
26 0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
28 0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30 0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31 0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33 Shadow byte legend (one shadow byte represents 8 application bytes):
34 Addressable:          00
35 Partially addressable: 01 02 03 04 05 06 07
36 Heap left redzone:    fa
37 Freed heap region:    fd
38 Stack left redzone:   f1
39 Stack mid redzone:    f2
40 Stack right redzone:  f3
41 Stack after return:   f5
42 Stack use after scope: f8
43 Global redzone:       f9
44 Global init order:    f6
45 Poisoned by user:     f7
46 Container overflow:   fc
47 Array cookie:         ac
48 Intra object redzone: bb
49 ASan internal:        fe
50 Left alloca redzone:  ca
51 Right alloca redzone: cb
52 Shadow gap:          cc
53 ==110920==ABORTING

```

 sample file :

https://drive.google.com/file/d/1GzEsD9U0bzjq9_Wi2i4f8yVTLA-gzgd8/view?usp=sharing

 crash info

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/
9      #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11 0x608000000178 is located 0 bytes to the right of 88-byte region [0x608000000120,0x60
12 allocated by thread T0 here:
13      #0 0x4aecdc8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc8)
14      #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
15
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18      0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
19      0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20      0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21      0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
22      0x0c107fff8010: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
23 =>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00[fa]
24      0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25      0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26      0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27      0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28      0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30 Addressable:                00
31 Partially addressable: 01 02 03 04 05 06 07
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
38 Stack use after scope:      f8
39 Global redzone:             f9
40 Global init order:          f6
41 Poisoned by user:           f7
42 Container overflow:         fc
43 Array cookie:               ac
44 Intra object redzone:       bb
45 ASan internal:              fe
46 Left alloca redzone:        ca
47 Right alloca redzone:       cb
48 Shadow gap:                 cc
49 ==112565==ABORTING

```

 sample file :

<https://drive.google.com/file/d/1is411Z2h-rU5Yq4rHBjhw2c7Cpi1C7U4/view?usp=sharing>

 crash info

gradle



```
1  ==112975==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
2  READ of size 1 at 0x6120000005cb thread T0
3      #0 0x6b55af (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b55af)
4      #1 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
5      #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 0x7fc4b3c13c86 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 0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
12 allocated by thread T0 here:
13      #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc)
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 0x7fc4b3c13c86 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 00 00 00 00 00 00 00 00
22   0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
24   0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
25   0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26 =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
27   0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 Shadow byte legend (one shadow byte represents 8 application bytes):
33   Addressable:           00
34   Partially addressable: 01 02 03 04 05 06 07
35   Heap left redzone:      fa
36   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:  f8
42   Global redzone:         f9
43   Global init order:      f6
44   Poisoned by user:       f7
45   Container overflow:     fc
46   Array cookie:           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

```

🔗 sample file :

https://drive.google.com/file/d/1_KAm-VI_nxWaT2nlyEraZSU9lfgclzF0/view?usp=sharing

🔗 crash info

gradle



```

1  ==113407==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f18b85fb808 at
2  READ of size 8 at 0x7f18b85fb808 thread T0
3      #0 0x6c08a6 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c08a6)
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 0x7f18bbbcac86 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 0x7f18b85fb808 is located 8 bytes to the right of 1048576-byte region [0x7f18b84fb800
11 allocated by thread T0 here:
12      #0 0x4aecdc8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc8)
13      #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
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 0x7f18bbbcac86 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 Shadow bytes around the buggy address:
20   0x0fe3970b76b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0fe3970b76c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0fe3970b76d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0fe3970b76e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24   0x0fe3970b76f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25  =>0x0fe3970b7700: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0fe3970b7710: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0fe3970b7720: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0fe3970b7730: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0fe3970b7740: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0fe3970b7750: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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:    fa

```

```

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

```

🔗 sample file :

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

🔗 crash info

gradle



```

1  =====
2  ==113825==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
3  READ of size 1 at 0x6120000005cb thread T0
4      #0 0x6b84b1 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b84b1)
5      #1 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
6      #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
7      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
8      #4 0x7f8d208dcc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9      #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11 0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
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      #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 0x7f8d208dcc86 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 00 00 00 00 00 00 00
22     0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

```

23 0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
24 0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
25 0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26 =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
27 0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28 0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30 0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31 0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 Shadow byte legend (one shadow byte represents 8 application bytes):
33 Addressable:          00
34 Partially addressable: 01 02 03 04 05 06 07
35 Heap left redzone:    fa
36 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: f8
42 Global redzone:       f9
43 Global init order:    f6
44 Poisoned by user:     f7
45 Container overflow:   fc
46 Array cookie:         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 ==113825==ABORTING

```

 sample file :

<https://drive.google.com/file/d/18HcVR2pHdUKdmdG99VyD42CkDEp8vDfR/view?usp=sharing>

 crash info

gradle



```

1 ==114199==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000295 at
2 READ of size 1 at 0x603000000295 thread T0
3 #0 0x6b03b5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b03b5)
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 0x7f60e4d53c86 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 0x603000000295 is located 0 bytes to the right of 21-byte region [0x603000000280,0x60
12 allocated by thread T0 here:
13     #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc
14     #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
15
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18     0x0c067fff8000: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
19     0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
20     0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 00 fa fa fd fd fd fa
21     0x0c067fff8030: fa fa fd fd fd fa fa fa 00 00 06 fa fa fa fd fd
22     0x0c067fff8040: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
23 =>0x0c067fff8050: 00 00[05]fa fa fa 00 00 00 fa fa fa fa fa fa fa
24     0x0c067fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25     0x0c067fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26     0x0c067fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27     0x0c067fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28     0x0c067fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30     Addressable:           00
31     Partially addressable: 01 02 03 04 05 06 07
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
38     Stack use after scope:  f8
39     Global redzone:         f9
40     Global init order:      f6
41     Poisoned by user:       f7
42     Container overflow:     fc
43     Array cookie:           ac
44     Intra object redzone:    bb
45     ASan internal:          fe
46     Left alloca redzone:    ca
47     Right alloca redzone:   cb
48     Shadow gap:             cc
49 ==114199==ABORTING

```

 sample file :

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

 crash info



gradle

```
1 ==114606==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60800000178 at
2 READ of size 1 at 0x60800000178 thread T0
3   #0 0x6b04de (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b04de)
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 0x7ff6deb1dc86 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 0x60800000178 is located 0 bytes to the right of 88-byte region [0x60800000120,0x60
12 allocated by thread T0 here:
13   #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8
14   #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
15
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18   0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
19   0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0c107fff8010: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
23 =>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00[fa]
24   0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30   Addressable:           00
31   Partially addressable: 01 02 03 04 05 06 07
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
38   Stack use after scope:  f8
39   Global redzone:         f9
40   Global init order:      f6
41   Poisoned by user:       f7
42   Container overflow:     fc
43   Array cookie:           ac
44   Intra object redzone:   bb
45   ASan internal:          fe
46   Left alloca redzone:    ca
47   Right alloca redzone:   cb
```



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

 sample file :

https://drive.google.com/file/d/1lh3_DS7REltISQaQyLkNDfoeC1APjlrC/view?usp=sharing

 crash info

gradle



```
1 ==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)
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 0x7fc6f9544c86 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 0x602000000519 is located 0 bytes to the right of 9-byte region [0x602000000510,0x602
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
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18 0x0c047fff8050: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
19 0x0c047fff8060: fa fa fd fa fa fa 00 00 fa fa 07 fa fa fa 00 fa
20 0x0c047fff8070: fa fa 07 fa fa fa 07 fa fa fa 07 fa fa fa 00 fa
21 0x0c047fff8080: fa fa 07 fa fa fa 07 fa fa fa 00 00 fa fa 00 fa
22 0x0c047fff8090: fa fa 05 fa fa fa 00 fa fa fa 00 00 fa fa 00 04
23 =>0x0c047fff80a0: fa fa 00[01]fa fa 02 fa fa fa 00 01 fa fa 07 fa
24 0x0c047fff80b0: fa fa 07 fa fa fa 00 fa fa fa 07 fa fa fa 00 00
25 0x0c047fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26 0x0c047fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27 0x0c047fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28 0x0c047fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30 Addressable: 00
31 Partially addressable: 01 02 03 04 05 06 07
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
```



```

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

```

sample file :

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

crash info

tap



```

1  ==115405==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000e0 at
2  READ of size 1 at 0x6070000000e0 thread T0
3      #0 0x617087 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x617087)
4      #1 0x4feb66 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
5      #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6      #3 0x7f93e83b7c86 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  0x6070000000e0 is located 0 bytes to the right of 80-byte region [0x607000000090,0x60
10 allocated by thread T0 here:
11      #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc
12      #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
14      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
15      #4 0x7f93e83b7c86 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      0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20      0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21      0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22      0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23      0x0c0e7fff8000: fa fa fa fa 00 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 00[fa]fa fa fa
25      0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
26      0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
27      0x0c0e7fff8040: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00

```




```

28 0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd
29 0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 fa
30 Shadow byte legend (one shadow byte represents 8 application bytes):
31 Addressable:          00
32 Partially addressable: 01 02 03 04 05 06 07
33 Heap left redzone:    fa
34 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: f8
40 Global redzone:        f9
41 Global init order:     f6
42 Poisoned by user:      f7
43 Container overflow:    fc
44 Array cookie:          ac
45 Intra object redzone:  bb
46 ASan internal:         fe
47 Left alloca redzone:   ca
48 Right alloca redzone:  cb
49 Shadow gap:           cc
50 ==115405==ABORTING

```

 sample file :

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

 crash info

gradle



```

1 ==115805==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6140000003cd at
2 READ of size 1 at 0x6140000003cd thread T0
3 #0 0x6b0d63 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0d63)
4 #1 0x6b256a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
5 #2 0x6b74c0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
6 #3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
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 0x7f3e2b577c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
10 #7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
11
12 0x6140000003cd is located 0 bytes to the right of 397-byte region [0x614000000240,0x6
13 allocated by thread T0 here:
14 #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8)
15 #1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
16 #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
20 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
21 Shadow bytes around the buggy address:
22   0x0c287fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0c287fff8030: 00 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   0x0c287fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26   0x0c287fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 =>0x0c287fff8070: 00 00 00 00 00 00 00 00 00 00[05]fa fa fa fa fa fa
28   0x0c287fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c287fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c287fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c287fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32   0x0c287fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33 Shadow byte legend (one shadow byte represents 8 application bytes):
34 Addressable:             00
35 Partially addressable: 01 02 03 04 05 06 07
36 Heap left redzone:      fa
37 Freed heap region:      fd
38 Stack left redzone:     f1
39 Stack mid redzone:      f2
40 Stack right redzone:    f3
41 Stack after return:     f5
42 Stack use after scope:  f8
43 Global redzone:         f9
44 Global init order:      f6
45 Poisoned by user:       f7
46 Container overflow:     fc
47 Array cookie:           ac
48 Intra object redzone:   bb
49 ASan internal:          fe
50 Left alloca redzone:    ca
51 Right alloca redzone:   cb
52 Shadow gap:             cc
53 ==115805==ABORTING

```

 sample file :

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

 crash info

tap



```

→ 1 ==116203==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000e0 at
  2 READ of size 1 at 0x6070000000e0 thread T0

```

```

3      #0 0x61731f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x61731f)
4      #1 0x4feb66 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
5      #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6      #3 0x7f448d7ccc86 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 0x6070000000e0 is located 0 bytes to the right of 80-byte region [0x607000000090,0x60
10 allocated by thread T0 here:
11      #0 0x4aecdc8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc8)
12      #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
14      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
15      #4 0x7f448d7ccc86 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 0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20 0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21 0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22 0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23 0x0c0e7fff8000: fa fa fa fa 00 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 00[fa]fa fa fa
25 0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
26 0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
27 0x0c0e7fff8040: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
28 0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd
29 0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 fa
30 Shadow byte legend (one shadow byte represents 8 application bytes):
31 Addressable:                00
32 Partially addressable: 01 02 03 04 05 06 07
33 Heap left redzone:          fa
34 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:       f8
40 Global redzone:              f9
41 Global init order:           f6
42 Poisoned by user:            f7
43 Container overflow:          fc
44 Array cookie:                ac
45 Intra object redzone:        bb
46 ASan internal:               fe
47 Left alloca redzone:         ca
48 Right alloca redzone:        cb
49 Shadow gap:                  cc
50 ==116203==ABORTING

```



🔗 sample file :

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

🔗 crash info

gradle



```
1  ==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 0x4febd8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4febd8)
5      #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6      #3 0x7f9e1c28bc86 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  0x603000000150 is located 0 bytes to the right of 32-byte region [0x603000000130,0x60
10 allocated by thread T0 here:
11      #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc
12      #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
14      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
15      #4 0x7f9e1c28bc86 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   0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
24 =>0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 00 00[fa]fa 00 00 04 fa
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 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
28   0x0c067fff8060: fa fa 00 00 02 fa fa fa 00 00 02 fa fa fa 00 00
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):
31   Addressable:           00
32   Partially addressable: 01 02 03 04 05 06 07
33   Heap left redzone:      fa
34   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:  f8
40   Global redzone:         f9
41   Global init order:      f6
```

```

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

```

🔗 sample file :

https://drive.google.com/file/d/1_PTp8gprryF4AwtMnMxqeYZjqZD5GE4v3/view?usp=sharing

🔗 crash info

gradle



```

1   ==101583==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6100000000f3 at
2   READ of size 1 at 0x6100000000f3 thread T0
3       #0 0x6b0478 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0478)
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 0x7f173ed37c86 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   0x6100000000f3 is located 0 bytes to the right of 179-byte region [0x610000000040,0x6
12   allocated by thread T0 here:
13       #0 0x4aecdb in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdb
14       #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
15
16   SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17   Shadow bytes around the buggy address:
18       0x0c207fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
19       0x0c207fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20       0x0c207fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21       0x0c207fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22       0x0c207fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
23   =>0x0c207fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00[03]fa
24       0x0c207fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25       0x0c207fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26       0x0c207fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27       0x0c207fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28       0x0c207fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   Shadow byte legend (one shadow byte represents 8 application bytes):
30   Addressable:          00

```

```

31 Partially addressable: 01 02 03 04 05 06 07
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
38 Stack use after scope:  f8
39 Global redzone:         f9
40 Global init order:      f6
41 Poisoned by user:       f7
42 Container overflow:     fc
43 Array cookie:           ac
44 Intra object redzone:   bb
45 ASan internal:          fe
46 Left alloca redzone:    ca
47 Right alloca redzone:   cb
48 Shadow gap:            cc
49 ==101583==ABORTING

```

sample file :

<https://drive.google.com/file/d/1ekBLM7xmf0heqwcs0e2abmzlqKE4CfRJ/view?usp=sharing>

crash info

gradle



```

1  ==102014==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f3d201e5808 at
2  READ of size 8 at 0x7f3d201e5808 thread T0
3      #0 0x6c0473 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0473)
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 0x7f3d24357c86 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 0x7f3d201e5808 is located 8 bytes to the right of 1048576-byte region [0x7f3d200e5800
11 allocated by thread T0 here:
12      #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
13      #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
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 0x7f3d24357c86 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 Shadow bytes around the buggy address:
→ 20  0x0fe824034ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

```

21 0x0fe824034ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22 0x0fe824034ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23 0x0fe824034ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24 0x0fe824034af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25 =>0x0fe824034b00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26 0x0fe824034b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27 0x0fe824034b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28 0x0fe824034b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 0x0fe824034b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30 0x0fe824034b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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:    fa
35 Freed heap region:    fd
36 Stack left redzone:    f1
37 Stack mid redzone:    f2
38 Stack right redzone:   f3
39 Stack after return:    f5
40 Stack use after scope: f8
41 Global redzone:        f9
42 Global init order:     f6
43 Poisoned by user:      f7
44 Container overflow:    fc
45 Array cookie:          ac
46 Intra object redzone:  bb
47 ASan internal:         fe
48 Left alloca redzone:   ca
49 Right alloca redzone:  cb
50 Shadow gap:            cc
51 ==102014==ABORTING

```

 sample file :

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

 crash info

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
11 allocated by thread T0 here:
12   #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc
13   #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
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 0x7fa28e8f7c86 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 Shadow bytes around the buggy address:
20   0x0ff4d14f4ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0ff4d14f4ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0ff4d14f4ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0ff4d14f4ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24   0x0ff4d14f4af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25 =>0x0ff4d14f4b00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0ff4d14f4b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0ff4d14f4b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0ff4d14f4b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0ff4d14f4b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0ff4d14f4b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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:      fa
35   Freed heap region:      fd
36   Stack left redzone:     f1
37   Stack mid redzone:      f2
38   Stack right redzone:    f3
39   Stack after return:     f5
40   Stack use after scope:   f8
41   Global redzone:         f9
42   Global init order:      f6
43   Poisoned by user:       f7
44   Container overflow:     fc
45   Array cookie:           ac
46   Intra object redzone:   bb
47   ASan internal:          fe
48   Left alloca redzone:    ca
49   Right alloca redzone:   cb
50   Shadow gap:             cc
51 ==102472==ABORTING

```

 sample file :

 <https://drive.google.com/file/d/1Vit9d-K4L6K45eDu-14fol9IVNCUN9y7/view?usp=sharing>

gradle



```

1  ==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)
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 0x7fb14c4a8c86 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 0x619000000418 is located 0 bytes to the right of 920-byte region [0x619000000080,0x6
12 allocated by thread T0 here:
13      #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8
14      #1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
15
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18   0x0c327fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
19   0x0c327fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c327fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c327fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0c327fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   =>0x0c327fff8080: 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
24   0x0c327fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0c327fff80b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
27   0x0c327fff80c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
28   0x0c327fff80d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30   Addressable:           00
31   Partially addressable: 01 02 03 04 05 06 07
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
38   Stack use after scope:   f8
39   Global redzone:         f9
40   Global init order:      f6
41   Poisoned by user:       f7
42   Container overflow:     fc
43   Array cookie:           ac
→ 44   Intra object redzone:   bb
45   ASan internal:          fe

```

```

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

```

🔗 sample file :

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

🔗 crash info

gradle



```

1  ==103532==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f98ea3af808 at
2  READ of size 8 at 0x7f98ea3af808 thread T0
3      #0 0x6c0a32 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0a32)
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 0x7f98f803ec86 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 0x7f98ea3af808 is located 8 bytes to the right of 1048576-byte region [0x7f98ea2af800
11 allocated by thread T0 here:
12      #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8)
13      #1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
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 0x7f98f803ec86 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 Shadow bytes around the buggy address:
20  0x0ff39d46deb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21  0x0ff39d46dec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22  0x0ff39d46ded0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23  0x0ff39d46dee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24  0x0ff39d46def0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25 =>0x0ff39d46df00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26  0x0ff39d46df10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27  0x0ff39d46df20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28  0x0ff39d46df30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29  0x0ff39d46df40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30  0x0ff39d46df50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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:          fa
35 Freed heap region:          fd

```

```

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

```

 sample file :

https://drive.google.com/file/d/1Vk_ulbbK5FYfeczsEU6YBQv7t8rAjvdA/view?usp=sharing

 crash info

gradle



```

1  ==104121==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x617000007110 at
2  READ of size 4 at 0x617000007110 thread T0
3      #0 0x6c0bc3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0bc3)
4      #1 0x6baee8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
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 0x7f987337ac86 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 0x617000007110 is located 392 bytes to the right of 648-byte region [0x617000006d00,0
12 freed by thread T0 here:
13      #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aee
14      #1 0x5add31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
15      #2 0x540f73 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540f73)
16      #3 0x6bc059 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bc059)
17      #4 0x6baee8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
18      #5 0x6baee8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
19      #6 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
20      #7 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
21      #8 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
22      #9 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
23

```

```

24 previously allocated by thread T0 here:
25     #0 0x4aeaa8 in realloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aeaa8)
26     #1 0x5add31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
27     #2 0x540696 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540696)
28     #3 0x6bda43 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bda43)
29     #4 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
30     #5 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
31     #6 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
32     #7 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
33
34 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
35 Shadow bytes around the buggy address:
36     0x0c2e7fff8dd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
37     0x0c2e7fff8de0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
38     0x0c2e7fff8df0: fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
39     0x0c2e7fff8e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
40     0x0c2e7fff8e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
41 =>0x0c2e7fff8e20: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
42     0x0c2e7fff8e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
43     0x0c2e7fff8e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
44     0x0c2e7fff8e50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
45     0x0c2e7fff8e60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
46     0x0c2e7fff8e70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
47 Shadow byte legend (one shadow byte represents 8 application bytes):
48 Addressable:                00
49 Partially addressable: 01 02 03 04 05 06 07
50 Heap left redzone:          fa
51 Freed heap region:          fd
52 Stack left redzone:         f1
53 Stack mid redzone:          f2
54 Stack right redzone:        f3
55 Stack after return:         f5
56 Stack use after scope:      f8
57 Global redzone:             f9
58 Global init order:          f6
59 Poisoned by user:           f7
60 Container overflow:         fc
61 Array cookie:               ac
62 Intra object redzone:       bb
63 ASan internal:              fe
64 Left alloca redzone:        ca
65 Right alloca redzone:       cb
66 Shadow gap:                 cc
67 ==104121==ABORTING

```

 sample file :



crash info

gradle



```
1  ==104506==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6080000017a at
2  WRITE of size 1 at 0x6080000017a thread T0
3      #0 0x6e412a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e412a)
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 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
10 0x6080000017a is located 0 bytes to the right of 90-byte region [0x60800000120,0x60
11 allocated by thread T0 here:
12      #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc
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
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18   0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
19   0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c107fff8000: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
22   0x0c107fff8010: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 01
23 =>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00[02]
24   0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30   Addressable:           00
31   Partially addressable: 01 02 03 04 05 06 07
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
38   Stack use after scope:  f8
39   Global redzone:         f9
40   Global init order:      f6
41   Poisoned by user:       f7
42   Container overflow:     fc
```

```

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

```

🔗 sample file :

<https://drive.google.com/file/d/1ObToO-dwTYTBCiAxxkB4MSu7N8Vu6Nd0/view?usp=sharing>

🔗 crash info

gradle



```

1  ==104877==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b00000db3 at
2  WRITE of size 176 at 0x60b00000db3 thread T0
3      #0 0x4adcdb in __asan_memset (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
4      #1 0x5cd359 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5cd359)
5      #2 0x4fea8d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fea8d)
6      #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/
8      #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
9
10 0x60b00000db3 is located 0 bytes to the right of 99-byte region [0x60b00000d50,0x60
11 allocated by thread T0 here:
12      #0 0x4aecdb in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdb
13      #1 0x5cd14f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5cd14f)
14      #2 0x4fea8d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fea8d)
15      #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
16      #4 0x7f604b90ec86 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 Shadow bytes around the buggy address:
20   0x0c167fff8160: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
21   0x0c167fff8170: fd fd fd fd fd fa fa fa fa fa fa fa fa fd fd
22   0x0c167fff8180: fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
23   0x0c167fff8190: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd
24   0x0c167fff81a0: fd fa fa fa fa fa fa fa fa fa 00 00 00 00 00
25 =>0x0c167fff81b0: 00 00 00 00 00 00[03]fa fa fa fa fa fa fa fa
26   0x0c167fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0c167fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c167fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c167fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c167fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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:      fa
35 Freed heap region:      fd
36 Stack left redzone:     f1
37 Stack mid redzone:      f2
38 Stack right redzone:    f3
39 Stack after return:     f5
40 Stack use after scope:   f8
41 Global redzone:         f9
42 Global init order:      f6
43 Poisoned by user:       f7
44 Container overflow:     fc
45 Array cookie:           ac
46 Intra object redzone:   bb
47 ASan internal:          fe
48 Left alloca redzone:    ca
49 Right alloca redzone:   cb
50 Shadow gap:             cc
51 ==104877==ABORTING

```

sample file :

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

crash info

gradle



```

1  ==105392==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000030bc3 at
2  WRITE of size 1 at 0x611000030bc3 thread T0
3      #0 0x6e41a8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41a8)
4      #1 0x5bea45 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)
5      #2 0x4fbdd4 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbdd4)
6      #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
7      #4 0x7f34f993dc86 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 0x611000030bc3 is located 0 bytes to the right of 195-byte region [0x611000030b00,0x6
11 allocated by thread T0 here:
12      #0 0x4aecdd in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdd
13      #1 0x6e3519 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
14      #2 0x5bea45 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)
15
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18 0x0c227fffe120: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
19 0x0c227fffe130: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
20 0x0c227fffe140: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd

```




```

21 0x0c227fffe150: fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa
22 0x0c227fffe160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23 =>0x0c227fffe170: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa fa fa
24 0x0c227fffe180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25 0x0c227fffe190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26 0x0c227fffe1a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27 0x0c227fffe1b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28 0x0c227fffe1c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30 Addressable:          00
31 Partially addressable: 01 02 03 04 05 06 07
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
38 Stack use after scope: f8
39 Global redzone:        f9
40 Global init order:     f6
41 Poisoned by user:      f7
42 Container overflow:    fc
43 Array cookie:          ac
44 Intra object redzone:  bb
45 ASan internal:         fe
46 Left alloca redzone:   ca
47 Right alloca redzone:  cb
48 Shadow gap:            cc
49 ==105392==ABORTING

```

 sample file :

https://drive.google.com/file/d/1Wl9wJ79lXESlfl4ycvNzE-kN8_AJlX9k/view?usp=sharing

 crash info

gradle



```

1 ==105898==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000ec2 at
2 WRITE of size 1 at 0x616000000ec2 thread T0
3 #0 0x6e41b0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b0)
4 #1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
5 #2 0x4fbe60 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60)
6 #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
7 #4 0x7fd2baafcc86 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 0x616000000ec2 is located 0 bytes to the right of 578-byte region [0x616000000c80,0x6

```



```

11 allocated by thread T0 here:
12     #0 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8)
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
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18     0x0c2c7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
19     0x0c2c7fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20     0x0c2c7fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21     0x0c2c7fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22     0x0c2c7fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23 =>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa fa fa
24     0x0c2c7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25     0x0c2c7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26     0x0c2c7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27     0x0c2c7fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28     0x0c2c7fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30 Addressable:             00
31 Partially addressable: 01 02 03 04 05 06 07
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
38 Stack use after scope:  f8
39 Global redzone:         f9
40 Global init order:      f6
41 Poisoned by user:       f7
42 Container overflow:     fc
43 Array cookie:           ac
44 Intra object redzone:   bb
45 ASan internal:          fe
46 Left alloca redzone:    ca
47 Right alloca redzone:   cb
48 Shadow gap:             cc
49 ==105898==ABORTING

```

🔗 sample file :

<https://drive.google.com/file/d/10HnRIC6e-FAFZnKpQjZengXfKKvlzj-Q/view?usp=sharing>

🔗 crash info

➔ gradle



```

1  ==106312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61600000ec2 at
2  WRITE of size 1 at 0x61600000ec2 thread T0
3      #0 0x6e41b8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b8)
4      #1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
5      #2 0x4fbe60 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60)
6      #3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
7      #4 0x7f5a9e97cc86 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 0x61600000ec2 is located 0 bytes to the right of 578-byte region [0x61600000c80,0x6
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
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18   0x0c2c7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
19   0x0c2c7fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c2c7fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c2c7fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0c2c7fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23 =>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa fa fa
24   0x0c2c7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c2c7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0c2c7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0c2c7fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c2c7fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30   Addressable:           00
31   Partially addressable: 01 02 03 04 05 06 07
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
38   Stack use after scope:  f8
39   Global redzone:         f9
40   Global init order:      f6
41   Poisoned by user:       f7
42   Container overflow:     fc
43   Array cookie:           ac
44   Intra object redzone:   bb
45   ASan internal:          fe
46   Left alloca redzone:    ca
47   Right alloca redzone:   cb
→ 48   Shadow gap:            cc
49  ==106312==ABORTING

```

🔗 sample file :

https://drive.google.com/file/d/1lrGT3ll8CXwJXYvPj57JUDs_FAO2k_MT/view?usp=sharing

🔗 crash info

gradle



```
1  ==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/
8      #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 0x4aec8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aec8
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
16 SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
17 Shadow bytes around the buggy address:
18   0x0c1c7fff8010: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
19   0x0c1c7fff8020: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
20   0x0c1c7fff8030: fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa
21   0x0c1c7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0c1c7fff8050: 00 00 00 02 fa fa fa fa fa fa fa fa 00 00 00 00
23 =>0x0c1c7fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[03]
24   0x0c1c7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
25   0x0c1c7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0c1c7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0c1c7fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c1c7fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29 Shadow byte legend (one shadow byte represents 8 application bytes):
30   Addressable:                00
31   Partially addressable: 01 02 03 04 05 06 07
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
38   Stack use after scope:      f8
39   Global redzone:             f9
```



```

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

```

 sample file :

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

 crash info

gradle



```

1  ==107517==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b000000660 at
2  READ of size 1 at 0x61b000000660 thread T0
3      #0 0x65fc97 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65fc97)
4      #1 0x4fe89d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
5      #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
6      #3 0x7fe052acac86 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  0x61b000000660 is located 0 bytes to the right of 1504-byte region [0x61b000000080,0x
10 allocated by thread T0 here:
11      #0 0x4aecdc in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecdc)
12      #1 0x4fa78f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
13      #2 0x4f9a31 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
14      #3 0x4f55dc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
15      #4 0x7fe052acac86 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   0x0c367fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0c367fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
21   0x0c367fff8090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0c367fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0c367fff80b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24 => 0x0c367fff80c0: 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
25   0x0c367fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
26   0x0c367fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
27   0x0c367fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c367fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c367fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```

```

30 Shadow byte legend (one shadow byte represents 8 application bytes):
31   Addressable:           00
32   Partially addressable: 01 02 03 04 05 06 07
33   Heap left redzone:      fa
34   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:  f8
40   Global redzone:         f9
41   Global init order:      f6
42   Poisoned by user:       f7
43   Container overflow:     fc
44   Array cookie:           ac
45   Intra object redzone:   bb
46   ASan internal:          fe
47   Left alloca redzone:    ca
48   Right alloca redzone:   cb
49   Shadow gap:             cc
50 ==107517==ABORTING

```

 sample file :

<https://drive.google.com/file/d/19NCya7nuaUHR5XMLNyDcfD-bKCvqnFL-/view?usp=sharing>

 crash info

gradle



```

1  ==108318==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
2  READ of size 1 at 0x6120000005cb thread T0
3      #0 0x6b544e (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b544e)
4      #1 0x6b6bf3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6bf3)
5      #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 0x7f0873f24c86 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 0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
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      #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 0x7f0873f24c86 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 00 00 00 00 00 00 00 00
22   0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
24   0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
25   0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26 =>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
27   0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
28   0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
29   0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
30   0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
31   0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
32 Shadow byte legend (one shadow byte represents 8 application bytes):
33   Addressable:           00
34   Partially addressable: 01 02 03 04 05 06 07
35   Heap left redzone:      fa
36   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:  f8
42   Global redzone:         f9
43   Global init order:      f6
44   Poisoned by user:       f7
45   Container overflow:     fc
46   Array cookie:           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 ==108318==ABORTING

```



catalogue 2: Vulnerability type – global heap buffer overflow

 sample file :

<https://drive.google.com/file/d/1q4YevANr8ZSFnWHb1RLY34u3BIil7K3J/view?usp=sharing>

 crash info

→ tap



```

1  ==15097==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000075fb88 at
2  READ of size 4 at 0x00000075fb88 thread T0
3      #0 0x718693 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x718693)
4      #1 0x6f835d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6f835d)
5      #2 0x4f5ad3 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5ad3)
6      #3 0x7f69023d2c86 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  0x00000075fb88 is located 56 bytes to the left of global variable 'cDigitsLut' define
10 0x00000075fb88 is located 0 bytes to the right of global variable 'kPow10' defined in
11 SUMMARY: AddressSanitizer: global-buffer-overflow (/home/bupt/Desktop/otfcc/bin/relea
12 Shadow bytes around the buggy address:
13   0x0000800e3f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
14   0x0000800e3f30: 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9
15   0x0000800e3f40: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
16   0x0000800e3f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
17   0x0000800e3f60: 00 00 00 00 00 06 f9 f9 f9 f9 f9 f9 00 00 00
18 =>0x0000800e3f70: 00[f9]f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00
19   0x0000800e3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20   0x0000800e3f90: 00 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00
21   0x0000800e3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22   0x0000800e3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
23   0x0000800e3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24 Shadow byte legend (one shadow byte represents 8 application bytes):
25   Addressable:                00
26   Partially addressable: 01 02 03 04 05 06 07
27   Heap left redzone:          fa
28   Freed heap region:          fd
29   Stack left redzone:         f1
30   Stack mid redzone:          f2
31   Stack right redzone:        f3
32   Stack after return:         f5
33   Stack use after scope:      f8
34   Global redzone:             f9
35   Global init order:          f6
36   Poisoned by user:           f7
37   Container overflow:         fc
38   Array cookie:               ac
39   Intra object redzone:       bb
40   ASan internal:              fe
41   Left alloca redzone:        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



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

sample file :

<https://drive.google.com/file/d/1xdw71uUMvagCwPort6Uh6uktU67Jgreg/view?usp=sharing>

crash info

gradle



```
1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==9104==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x0000004
4 ==9104==The signal is caused by a READ memory access.
5 ==9104==Hint: address points to the zero page.
➔ 6 #0 0x4fbc0b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbc0b)
```

```

7      #1 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
8      #2 0x7fada3943c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9      #3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11 AddressSanitizer can not provide additional info.
12 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
13 ==9104==ABORTING

```

 sample file :

https://drive.google.com/file/d/1UuJo7ifneTeY5j_ZILPG4y8XqAlUm2eE/view?usp=sharing

 crash info

routeros



```

1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==10580==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x000000
4 ==10580==The signal is caused by a READ memory access.
5 ==10580==Hint: address points to the zero page.
6 ==10580==WARNING: failed to fork (errno 12)
7 ==10580==WARNING: failed to fork (errno 12)
8 ==10580==WARNING: failed to fork (errno 12)
9 ==10580==WARNING: failed to fork (errno 12)
10 ==10580==WARNING: failed to fork (errno 12)
11 ==10580==WARNING: Failed to use and restart external symbolizer!
12      #0 0x4fe9a7 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe9a7)
13      #1 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
14      #2 0x7f16ea646c86 (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
15      #3 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 ==10580==ABORTING

```

 sample file :

https://drive.google.com/file/d/1OrlHDs0V6s2DrbjcYwWAoF2kd2_fao7M/view?usp=sharing

 crash info

gradle



```

1 AddressSanitizer:DEADLYSIGNAL
2 =====
→ 3 ==128856==ERROR: AddressSanitizer: SEGV on unknown address 0x612000096e63 (pc 0x7fdeb

```

```

4  ==128856==The signal is caused by a READ memory access.
5      #0 0x7fdeb5ff1384 /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86_64/multiarch
6      #1 0x4ad6eb in __asan_memcpy (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4ad6eb)
7      #2 0x6b53ed (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
8      #3 0x6b6b99 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
9      #4 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
10     #5 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
11     #6 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
12     #7 0x7fdeb5f57c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc.so.6+0x7fdeb5f57c86
13     #8 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
14
15 AddressSanitizer can not provide additional info.
16 SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86_64/multiarch
17 ==128856==ABORTING

```

 sample file :

<https://drive.google.com/file/d/1tkNyCltr6mhLx2Um1ZsyAthH55DCIW/view?usp=sharing>

 crash info

gradle



```

1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==130785==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x000000000000)
4 ==130785==The signal is caused by a READ memory access.
5 ==130785==Hint: address points to the zero page.
6 ==130785==WARNING: failed to fork (errno 12)
7 ==130785==WARNING: failed to fork (errno 12)
8 ==130785==WARNING: failed to fork (errno 12)
9 ==130785==WARNING: failed to fork (errno 12)
10 ==130785==WARNING: failed to fork (errno 12)
11 ==130785==WARNING: Failed to use and restart external symbolizer!
12     #0 0x5266a8 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5266a8)
13     #1 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
14     #2 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
15     #3 0x7f952a4e0c86 (/lib/x86_64-linux-gnu/libc.so.6+0x7f952a4e0c86)
16     #4 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
17
18 AddressSanitizer can not provide additional info.
19 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
20 ==130785==ABORTING

```

 sample file :

 <https://drive.google.com/file/d/1Qx1K-BhcvLipRDmM1nNUq8t1STWpJLDz/view?usp=sharing>

crash info

gradle



```
1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==1197==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000004cc (pc 0x00000006
4 ==1197==The signal is caused by a READ memory access.
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)
8   #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
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/
11  #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
12
13 AddressSanitizer can not provide additional info.
14 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
15 ==1197==ABORTING
```

sample file :

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

crash info

gradle



```
1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==2966==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000036 (pc 0x00000004
4 ==2966==The signal is caused by a READ memory access.
5 ==2966==Hint: address points to the zero page.
6   #0 0x4fbbb6 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbbb6)
7   #1 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
8   #2 0x7f3e141cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9   #3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11 AddressSanitizer can not provide additional info.
12 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
13 ==2966==ABORTING
```

sample file :

https://drive.google.com/file/d/18tbZsfm_CgaAoB5L_22EFCF_DWTYrAVg/view?usp=sharing

crash info

gradle



```
1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==3991==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000036 (pc 0x00000004
4 ==3991==The signal is caused by a READ memory access.
5 ==3991==Hint: address points to the zero page.
6     #0 0x4fe954 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe954)
7     #1 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
8     #2 0x7fee2bb48c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9     #3 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
10
11 AddressSanitizer can not provide additional info.
12 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
13 ==3991==ABORTING
```

sample file :

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

crash info

gradle



```
1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==8370==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000000704 (pc 0x00000006
4 ==8370==The signal is caused by a READ memory access.
5 ==8370==Hint: address points to the zero page.
6     #0 0x6babea (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6babea)
7     #1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
8     #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
9     #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
10    #4 0x7f8358612c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
11    #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
12
13 AddressSanitizer can not provide additional info.
14 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
15 ==8370==ABORTING
```

sample file :

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

crash info

→ gradle



```

1 AddressSanitizer:DEADLYSIGNAL
2 =====
3 ==9840==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000006
4 ==9840==The signal is caused by a READ memory access.
5 ==9840==Hint: address points to the zero page.
6   #0 0x6b6a8f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6a8f)
7   #1 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
8   #2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
9   #3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
10  #4 0x7f4071149c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
11  #5 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
12
13 AddressSanitizer can not provide additional info.
14 SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
15 ==9840==ABORTING

```

 sample file :

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

 crash info

gradle



```

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

```

 sample file :

https://drive.google.com/file/d/1v5-qJeZpmw7_txAnhl8ew82NW2BCdLFH/view?usp=sharing

 crash info



gradle

```
1 =====
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/
8   #4 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 ==1985==ABORTING
```

🔗 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



```
1 ./otfccbuild -O3 -q --force-cid [sample file] -o /dev/null
```

🔗 crash info

shell



```
1 ==49487==ERROR: AddressSanitizer: heap-use-after-free on address 0x603000000011 at pc
2 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
5   #2 0x72a75e (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x72a75e)
6   #3 0x72afc2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x72afc2)
7   #4 0x4f65ac (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4f65ac)
8   #5 0x7f6e50b86c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
9   #6 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x41c549)
10
11 0x603000000011 is located 1 bytes inside of 20-byte region [0x603000000010,0x60300000
➔12 freed by thread T0 here:
```



```

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)
15      #2 0x7f6e50b86c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
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
21 SUMMARY: AddressSanitizer: heap-use-after-free (/home/bupt/Desktop/otfcc/bin/release-
22 Shadow bytes around the buggy address:
23      0x0c067fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
24      0x0c067fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25      0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26      0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27      0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
28 =>0x0c067fff8000: fa fa[fd]fd fd fa fa fa fd fd fd fa fa fa fd fd
29      0x0c067fff8010: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
30      0x0c067fff8020: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
31      0x0c067fff8030: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fa fa
32      0x0c067fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
33      0x0c067fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
34 Shadow byte legend (one shadow byte represents 8 application bytes):
35 Addressable:                00
36 Partially addressable: 01 02 03 04 05 06 07
37 Heap left redzone:          fa
38 Freed heap region:          fd
39 Stack left redzone:          f1
40 Stack mid redzone:           f2
41 Stack right redzone:         f3
42 Stack after return:          f5
43 Stack use after scope:       f8
44 Global redzone:              f9
45 Global init order:           f6
46 Poisoned by user:            f7
47 Container overflow:          fc
48 Array cookie:                ac
49 Intra object redzone:        bb
50 ASan internal:               fe
51 Left alloca redzone:         ca
52 Right alloca redzone:        cb
53 Shadow gap:                  cc
54 ==49487==ABORTING

```



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.

CVE

©2022 By Victory+

Victory+ ♥ TBaozi



Local search

Search for Posts



Powered by [hexo-generator-search](#)

✕

