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

```
./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

crash info

gradle

```
==100398==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
READ of size 4294967295 at 0x61200000044b thread T0
    #0 0x4adb11 in __asan_memcpy (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
    #1 0x6b53ed  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
    #2 0x6b6b99  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
    #3 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #4 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #5 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #6 0x7f6a7f4b6c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #7 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f6a7f4b6c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8050: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
```

```
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==100398==ABORTING
```

sample file :

https://drive.google.com/file/d/1BZ_T5C1cPfYgvueIBJ8vu45zZcSNhJAt/view?usp=sharing

crash info

gradle

```
=================================================================
==111746==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
READ of size 1 at 0x61200000044b thread T0
    #0 0x6b558f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b558f)
    #1 0x6b6bf3  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6bf3)
    #2 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7ff49f52ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7ff49f52ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8050: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==111746==ABORTING
```

sample file :

https://drive.google.com/file/d/1Tm4VQLzEsHYm-VZm-8S3Ii854wnKpgby/view?usp=sharing

crash info

gradle

```
=================================================================
==117024==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000832 at
READ of size 1 at 0x616000000832 thread T0
    #0 0x6e7e3d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e7e3d)
    #1 0x5eb58a  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb58a)
    #2 0x4fe227  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fcd6ac0dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x616000000832 is located 680 bytes to the right of 522-byte region [0x616000000380,0
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7fcd6ac0dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c2c7fff80b0: 00 02 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2c7fff8100: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==117024==ABORTING
```

sample file :

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

crash info

gradle

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

```
    #2 0x4fe227  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fdfdc8c8c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x616000000837 is located 685 bytes to the right of 522-byte region [0x616000000380,0
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7fdfdc8c8c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c2c7fff80b0: 00 02 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2c7fff8100: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==106716==ABORTING
```

➜

sample file :

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

crash info

gradle

```
=================================================================
==107908==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
READ of size 1 at 0x6120000005cb thread T0
    #0 0x6b5567  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b5567)
    #1 0x6b6b99  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
    #2 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7fc74767cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fc74767cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
```

```
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==107908==ABORTING
```

sample file :

https://drive.google.com/file/d/1CdfTd5Emf_jDRLv1z64W5Rm3O1Q1JTyQ/view?usp=sharing

crash info

gradle

```
==108759==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000616 at
READ of size 1 at 0x612000000616 thread T0
    #0 0x6b064d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b064d)
    #1 0x6b256a  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
    #2 0x6b74c0  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
    #3 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #4 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #5 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #6 0x7f93b614bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #7 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x612000000616 is located 75 bytes to the right of 267-byte region [0x6120000004c0,0x
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f93b614bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff80b0: 00 00 00 00 00 00 00 00 00 03 fa fa fa fa fa fa
=>0x0c247fff80c0: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==108759==ABORTING
```

sample file :

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

crash info

gradle

```
==109163==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000008bd at
READ of size 1 at 0x6120000008bd thread T0
    #0 0x6adb1e  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6adb1e)
    #1 0x6b71de  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b71de)
    #2 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7f199d870c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6120000008bd is located 754 bytes to the right of 267-byte region [0x6120000004c0,0
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
```

```
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f199d870c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c247fff8110: fa fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa
  0x0c247fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==109163==ABORTING
```

sample file :

https://drive.google.com/file/d/15zqWcqkig0fr36a7wOqurSItd1rq9n0_/view?usp=sharing

crash info

→ **gradle**

```
==109553==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000078a6 at
READ of size 1 at 0x6160000078a6 thread T0
    #0 0x6e20a0  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e20a0)
    #1 0x5eb5ec  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb5ec)
    #2 0x4fe227  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f2da0c05c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

Address 0x6160000078a6 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c2c7fff8ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8ed0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8ee0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2c7fff8f10: fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==109553==ABORTING
```

sample file :

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

crash info

gradle

```
==109939==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000001d6 at
READ of size 1 at 0x6020000001d6 thread T0
    #0 0x5e15d8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5e15d8)
    #1 0x4fe1e2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe1e2)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f502f9c0c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6020000001d6 is located 0 bytes to the right of 6-byte region [0x6020000001d0,0x602
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7f502f9c0c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 00 00 fa fa 00 03 fa fa fd fa fa fa 00 03
  0x0c047fff8010: fa fa fd fa fa fa 00 00 fa fa fd fa fa fa fd fa
  0x0c047fff8020: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
=>0x0c047fff8030: fa fa 04 fa fa fa 00 fa fa fa[06]fa fa fa fd fa
  0x0c047fff8040: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8050: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8060: fa fa fd fa fa fa 00 00 fa fa fa fa fa fa fa fa
  0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
```

```
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==109939==ABORTING
```

sample file :

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

crash info

gradle

```
==110431==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000044b at
READ of size 1 at 0x61200000044b thread T0
    #0 0x6b559f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b559f)
    #1 0x6b6d86  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6d86)
    #2 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7f17f472ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x61200000044b is located 0 bytes to the right of 267-byte region [0x612000000340,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f17f472ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8030: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8050: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff8080: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
```

```
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==110431==ABORTING
```

sample file :

https://drive.google.com/file/d/1COw6yyp8w99fEVhoeBz9mBw4h0_aZi_n/view?usp=sharing

crash info

gradle

```
==110920==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
READ of size 1 at 0x6120000005cb thread T0
    #0 0x6b0b2c  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0b2c)
    #1 0x6b256a  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
    #2 0x6b74c0  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
    #3 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #4 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #5 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #6 0x7f857d9cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #7 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f857d9cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
```

```
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==110920==ABORTING
```

sample file :

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

crash info

gradle

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

```
    #5 0x7f1fc338fc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x608000000178 is located 0 bytes to the right of 88-byte region [0x608000000120,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8010: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00[fa]
  0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==112565==ABORTING
```

sample file :

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

crash info

gradle

```
==112975==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
READ of size 1 at 0x6120000005cb thread T0
    #0 0x6b55af  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b55af)
    #1 0x6b6b99  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
    #2 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7fc4b3c13c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fc4b3c13c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
```

```
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==112975==ABORTING
```

sample file :

https://drive.google.com/file/d/1_KAm-Vl_nxWaT2nlyEraZSU9lfgclzF0/view?usp=sharing

crash info

gradle

```
==113407==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f18b85fb808 at
READ of size 8 at 0x7f18b85fb808 thread T0
    #0 0x6c08a6  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c08a6)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f18bbbcac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x7f18b85fb808 is located 8 bytes to the right of 1048576-byte region [0x7f18b84fb800
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x526fd2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f18bbbcac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0fe3970b76b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe3970b7700: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7710: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7720: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7730: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7740: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7750: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
```

```
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==113407==ABORTING
```

sample file :

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

crash info

gradle

```
=================================================================
==113825==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
READ of size 1 at 0x6120000005cb thread T0
    #0 0x6b84b1  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b84b1)
    #1 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f8d208dcc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f8d208dcc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==113825==ABORTING
```

sample file :

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

crash info

gradle

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

```
0x603000000295 is located 0 bytes to the right of 21-byte region [0x603000000280,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c067fff8000: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
  0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 00 fa fa fd fd fd fa
  0x0c067fff8030: fa fa fd fd fd fa fa fa 00 00 06 fa fa fa fd fd
  0x0c067fff8040: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
=>0x0c067fff8050: 00 00[05]fa fa fa 00 00 00 fa fa fa fa fa fa fa
  0x0c067fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==114199==ABORTING
```

sample file :

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

crash info

➔

gradle

```
==114606==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x608000000178 at
READ of size 1 at 0x608000000178 thread T0
    #0 0x6b04de  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b04de)
    #1 0x6b99ca  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
    #2 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7ff6deb1dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x608000000178 is located 0 bytes to the right of 88-byte region [0x608000000120,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8010: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00[fa]
  0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
```

➜

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

sample file :

https://drive.google.com/file/d/1lh3_DS7RElIlSQaQyLkNDfoeC1APjIrC/view?usp=sharing

crash info

gradle

```
==114999==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000519 at
READ of size 1 at 0x602000000519 thread T0
    #0 0x6b0466  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0466)
    #1 0x6b99ca  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
    #2 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7fc6f9544c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x602000000519 is located 0 bytes to the right of 9-byte region [0x602000000510,0x602
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c047fff8050: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8060: fa fa fd fa fa fa 00 00 fa fa 07 fa fa fa 00 fa
  0x0c047fff8070: fa fa 07 fa fa fa 07 fa fa fa 07 fa fa fa 00 fa
  0x0c047fff8080: fa fa 07 fa fa fa 07 fa fa fa 00 00 fa fa 00 fa
  0x0c047fff8090: fa fa 05 fa fa fa 00 fa fa fa 00 00 fa fa 00 04
=>0x0c047fff80a0: fa fa 00[01]fa fa 02 fa fa fa 00 01 fa fa 07 fa
  0x0c047fff80b0: fa fa 07 fa fa fa 00 fa fa fa 07 fa fa fa 00 00
  0x0c047fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
```

```
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==114999==ABORTING
```

sample file :

https://drive.google.com/file/d/1bk62xlR2SRqMNE9Q2lXDqDk54nGJZ6yl/view?usp=sharing

crash info

tap

```
==115405==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000e0 at
READ of size 1 at 0x6070000000e0 thread T0
    #0 0x617087  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x617087)
    #1 0x4feb66  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f93e83b7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6070000000e0 is located 0 bytes to the right of 80-byte region [0x607000000090,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7f93e83b7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 04 fa fa fa
=>0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
  0x0c0e7fff8040: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
```

```
  0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 00 fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==115405==ABORTING
```

sample file :

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

crash info

gradle

```
==115805==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6140000003cd at
READ of size 1 at 0x6140000003cd thread T0
    #0 0x6b0d63  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0d63)
    #1 0x6b256a  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
    #2 0x6b74c0  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
    #3 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #4 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #5 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #6 0x7f3e2b577c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #7 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6140000003cd is located 0 bytes to the right of 397-byte region [0x614000000240,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
```

```
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f3e2b577c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c287fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c287fff8030: 00 00 00 00 00 00 00 00 00 05 fa fa fa fa fa fa
  0x0c287fff8040: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c287fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c287fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c287fff8070: 00 00 00 00 00 00 00 00 00[05]fa fa fa fa fa fa
  0x0c287fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==115805==ABORTING
```

sample file :

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

crash info

tap

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

```
    #0 0x61731f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x61731f)
    #1 0x4feb66  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f448d7ccc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6070000000e0 is located 0 bytes to the right of 80-byte region [0x607000000090,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7f448d7ccc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 04 fa fa fa
=>0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00[fa]fa fa fa
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
  0x0c0e7fff8040: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 00 fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==116203==ABORTING
```

sample file :

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

crash info

gradle

```
==116615==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000150 at
READ of size 1 at 0x603000000150 thread T0
    #0 0x6171b2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6171b2)
    #1 0x4febdc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4febdc)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f9e1c28bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x603000000150 is located 0 bytes to the right of 32-byte region [0x603000000130,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7f9e1c28bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff8000: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
=>0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 00[fa]fa 00 00 04 fa
  0x0c067fff8030: fa fa 00 00 00 00 fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8040: fd fa fa fa 00 00 06 fa fa fa fd fd fd fa fa fa
  0x0c067fff8050: 00 00 00 fa fa fa fd fd fd fd fa fa 00 00 02 fa
  0x0c067fff8060: fa fa 00 00 02 fa fa fa 00 00 02 fa fa fa 00 00
  0x0c067fff8070: 02 fa fa fa 00 00 02 fa fa fa 00 00 02 fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
```

```
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==116615==ABORTING
```

sample file :

https://drive.google.com/file/d/1_PTp8gpryF4AwtMnMxqeYZjqZD5GE4v3/view?usp=sharing

crash info

gradle

```
==101583==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6100000000f3 at
READ of size 1 at 0x6100000000f3 thread T0
    #0 0x6b0478  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0478)
    #1 0x6b99ca  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
    #2 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7f173ed37c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6100000000f3 is located 0 bytes to the right of 179-byte region [0x610000000040,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c207fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c207fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[03]fa
  0x0c207fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
```

```
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==101583==ABORTING
```

sample file :

https://drive.google.com/file/d/1ekBLM7xmf0heqwcs0e2abmzIqKE4CfRJ/view?usp=sharing

crash info

gradle

```
==102014==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f3d201e5808 at
READ of size 8 at 0x7f3d201e5808 thread T0
    #0 0x6c0473  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0473)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f3d24357c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x7f3d201e5808 is located 8 bytes to the right of 1048576-byte region [0x7f3d200e5800
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x526fd2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f3d24357c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0fe824034ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0fe824034ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe824034ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe824034ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe824034af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe824034b00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe824034b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe824034b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe824034b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe824034b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe824034b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==102014==ABORTING
```

sample file :

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

crash info

gradle

```
==102472==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fa28a7e5808 at
READ of size 8 at 0x7fa28a7e5808 thread T0
    #0 0x6c0414  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0414)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fa28e8f7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
```

```
0x7fa28a7e5808 is located 8 bytes to the right of 1048576-byte region [0x7fa28a6e5800
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x526fd2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fa28e8f7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0ff4d14f4ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff4d14f4ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff4d14f4ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff4d14f4ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff4d14f4af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff4d14f4b00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4d14f4b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4d14f4b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4d14f4b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4d14f4b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4d14f4b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==102472==ABORTING
```

sample file :

https://drive.google.com/file/d/1Vit9d-K4L6K45eDu-14foI9IVNCUN9y7/view?usp=sharing

crash info

gradle

```
==102877==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000418 at
READ of size 1 at 0x619000000418 thread T0
    #0 0x6b05ce  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05ce)
    #1 0x6b99ca  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
    #2 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7fb14c4a8c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x619000000418 is located 0 bytes to the right of 920-byte region [0x619000000080,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c327fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8080: 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
```

```
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==102877==ABORTING
```

sample file :

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

crash info

gradle

```
==103532==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f98ea3af808 at
READ of size 8 at 0x7f98ea3af808 thread T0
    #0 0x6c0a32  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0a32)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f98f803ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x7f98ea3af808 is located 8 bytes to the right of 1048576-byte region [0x7f98ea2af800
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x526fd2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f98f803ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0ff39d46deb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff39d46dec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff39d46ded0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff39d46dee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff39d46def0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff39d46df00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff39d46df10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff39d46df20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff39d46df30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff39d46df40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff39d46df50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
```

```
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==103532==ABORTING
```

sample file :

https://drive.google.com/file/d/1Vk_uIbbK5FYfeczsEU6YBQv7t8rAjvdA/view?usp=sharing

crash info

gradle

```
==104121==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x617000007110 at
READ of size 4 at 0x617000007110 thread T0
    #0 0x6c0bc3  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0bc3)
    #1 0x6baee8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
    #2 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x617000007110 is located 392 bytes to the right of 648-byte region [0x617000006d00,0
freed by thread T0 here:
    #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aee
    #1 0x5add31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
    #2 0x540f73  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540f73)
    #3 0x6bc059  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bc059)
    #4 0x6baee8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
    #5 0x6baee8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
    #6 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #7 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #8 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #9 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

```

```
previously allocated by thread T0 here:
    #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aee
    #1 0x5add31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
    #2 0x540696  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540696)
    #3 0x6bda43  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bda43)
    #4 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #5 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #6 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #7 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c2e7fff8dd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e7fff8de0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e7fff8df0: fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2e7fff8e20: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==104121==ABORTING
```

sample file :

https://drive.google.com/file/d/1pcti9C8HAjg4JGBbYHrS0oENMQWp_zsl/view?usp=sharing

crash info

gradle

```
==104506==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60800000017a at
WRITE of size 1 at 0x60800000017a thread T0
    #0 0x6e412a  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e412a)
    #1 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
    #2 0x4fbe96  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe96)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7f034a2f9c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x60800000017a is located 0 bytes to the right of 90-byte region [0x608000000120,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6e3519  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
    #2 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8000: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c107fff8010: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 01
=>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00[02]
  0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
```

```
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==104506==ABORTING
```

sample file :

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

crash info

gradle

```
==104877==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b000000db3 at
WRITE of size 176 at 0x60b000000db3 thread T0
    #0 0x4adcdb in __asan_memset (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
    #1 0x5cd359  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5cd359)
    #2 0x4fea8d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fea8d)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f604b90ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x60b000000db3 is located 0 bytes to the right of 99-byte region [0x60b000000d50,0x60
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x5cd14f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5cd14f)
    #2 0x4fea8d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fea8d)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f604b90ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c167fff8160: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c167fff8170: fd fd fd fd fd fa fa fa fa fa fa fa fa fa fd fd
  0x0c167fff8180: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c167fff8190: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c167fff81a0: fd fa fa fa fa fa fa fa fa fa fa 00 00 00 00 00
=>0x0c167fff81b0: 00 00 00 00 00 00[03]fa fa fa fa fa fa fa fa fa
  0x0c167fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
```

```
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==104877==ABORTING
```

sample file :

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

crash info

gradle

```
==105392==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000030bc3 at
WRITE of size 1 at 0x611000030bc3 thread T0
    #0 0x6e41a8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41a8)
    #1 0x5bea45  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)
    #2 0x4fbdd4  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbdd4)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7f34f993dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x611000030bc3 is located 0 bytes to the right of 195-byte region [0x611000030b00,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6e3519  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
    #2 0x5bea45  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c227fffe120: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c227fffe130: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c227fffe140: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

```
  0x0c227fffe150: fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c227fffe170: 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa fa
  0x0c227fffe180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe1a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe1b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe1c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==105392==ABORTING
```

sample file :

https://drive.google.com/file/d/1Wl9wJ79IXESlfL4ycvNzE-kN8_AJlX9k/view?usp=sharing

crash info

gradle

```
==105898==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000ec2 at
WRITE of size 1 at 0x616000000ec2 thread T0
    #0 0x6e41b0  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b0)
    #1 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
    #2 0x4fbe60  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7fd2baafcc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x616000000ec2 is located 0 bytes to the right of 578-byte region [0x616000000c80,0x6
```

```
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6e3519  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
    #2 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c2c7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa fa
  0x0c2c7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==105898==ABORTING
```

sample file :

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

crash info

→ **gradle**

```
==106312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000ec2 at
WRITE of size 1 at 0x616000000ec2 thread T0
    #0 0x6e41b8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b8)
    #1 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
    #2 0x4fbe60  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7f5a9e97cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x616000000ec2 is located 0 bytes to the right of 578-byte region [0x616000000c80,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6e3519  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
    #2 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c2c7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa fa
  0x0c2c7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==106312==ABORTING
```

sample file :

https://drive.google.com/file/d/1lrGT3Il8CXwJXYvPj57JUDs_FAO2k_MT/view?usp=sharing

crash info

gradle

```
==107115==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60e00000037b at
WRITE of size 1 at 0x60e00000037b thread T0
    #0 0x6e420d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e420d)
    #1 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
    #2 0x4fbe96  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe96)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7f3dd47a6c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x60e00000037b is located 0 bytes to the right of 155-byte region [0x60e0000002e0,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6e3519  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
    #2 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c1c7fff8010: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c1c7fff8020: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1c7fff8030: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x0c1c7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff8050: 00 00 00 02 fa fa fa fa fa fa fa fa 00 00 00 00
=>0x0c1c7fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[03]
  0x0c1c7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
```

```
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==107115==ABORTING
```

sample file :

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

crash info

gradle

```
==107517==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b000000660 at
READ of size 1 at 0x61b000000660 thread T0
    #0 0x65fc97  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65fc97)
    #1 0x4fe89d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7fe052acac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x61b000000660 is located 0 bytes to the right of 1504-byte region [0x61b000000080,0x
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7fe052acac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c367fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff80b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c367fff80c0: 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
  0x0c367fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==107517==ABORTING
```

sample file :

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

crash info

gradle

```
==108318==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6120000005cb at
READ of size 1 at 0x6120000005cb thread T0
    #0 0x6b544e  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b544e)
    #1 0x6b6bf3  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6bf3)
    #2 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7f0873f24c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6120000005cb is located 0 bytes to the right of 267-byte region [0x6120000004c0,0x6
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd
    #1 0x6b69c5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f0873f24c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release
Shadow bytes around the buggy address:
  0x0c247fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff80b0: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c247fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==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

```
==15097==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000075fb88 at
READ of size 4 at 0x00000075fb88 thread T0
    #0 0x718693  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x718693)
    #1 0x6f835d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6f835d)
    #2 0x4f5ad3  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5ad3)
    #3 0x7f69023d2c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x00000075fb88 is located 56 bytes to the left of global variable 'cDigitsLut' define
0x00000075fb88 is located 0 bytes to the right of global variable 'kPow10' defined in
SUMMARY: AddressSanitizer: global-buffer-overflow (/home/bupt/Desktop/otfcc/bin/relea
Shadow bytes around the buggy address:
  0x0000800e3f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3f30: 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9
  0x0000800e3f40: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000800e3f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3f60: 00 00 00 00 00 06 f9 f9 f9 f9 f9 f9 00 00 00 00
=>0x0000800e3f70: 00[f9]f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
  0x0000800e3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3f90: 00 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
  0x0000800e3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==15097==ABORTING
```

catalogue 3: Vulnerability type – SEGV

sample file :

https://drive.google.com/file/d/1-sFx_eHoSXa79pye6Cdv2i2zvAfHwsGI/view?usp=sharing

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==6233==ERROR: AddressSanitizer: SEGV on unknown address 0x6120002ad5dd (pc 0x7fbef83
==6233==The signal is caused by a READ memory access.
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: Failed to use and restart external symbolizer!
    #0 0x7fbef8354384  (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
    #1 0x4ad6eb  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4ad6eb)
    #2 0x6b53ed  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
    #3 0x6b6d86  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6d86)
    #4 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #5 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #6 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #7 0x7fbef82bac86  (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #8 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
==6233==ABORTING
```

sample file :

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

crash info

gradle

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

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

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==9104==ABORTING
```

sample file :

https://drive.google.com/file/d/1UuJo7ifneTeY5j_ZILPG4y8XqAIUm2eE/view?usp=sharing

crash info

routeros

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==10580==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x000000
==10580==The signal is caused by a READ memory access.
==10580==Hint: address points to the zero page.
==10580==WARNING: failed to fork (errno 12)
==10580==WARNING: failed to fork (errno 12)
==10580==WARNING: failed to fork (errno 12)
==10580==WARNING: failed to fork (errno 12)
==10580==WARNING: failed to fork (errno 12)
==10580==WARNING: Failed to use and restart external symbolizer!
    #0 0x4fe9a7  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe9a7)
    #1 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #2 0x7f16ea646c86  (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #3 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==10580==ABORTING
```

sample file :

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

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==128856==ERROR: AddressSanitizer: SEGV on unknown address 0x612000096e63 (pc 0x7fdeb
```

```
==128856==The signal is caused by a READ memory access.
    #0 0x7fdeb5ff1384  /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86_64/multia
    #1 0x4ad6eb in __asan_memcpy (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+
    #2 0x6b53ed  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
    #3 0x6b6b99  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
    #4 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #5 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #6 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #7 0x7fdeb5f57c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #8 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86_
==128856==ABORTING
```

sample file :

https://drive.google.com/file/d/1tkNyCItred6mhLx2Um1ZsyAthH55DCIW/view?usp=sharing

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==130785==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x00000
==130785==The signal is caused by a READ memory access.
==130785==Hint: address points to the zero page.
==130785==WARNING: failed to fork (errno 12)
==130785==WARNING: failed to fork (errno 12)
==130785==WARNING: failed to fork (errno 12)
==130785==WARNING: failed to fork (errno 12)
==130785==WARNING: failed to fork (errno 12)
==130785==WARNING: Failed to use and restart external symbolizer!
    #0 0x5266a8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5266a8)
    #1 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f952a4e0c86  (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==130785==ABORTING
```

sample file :

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

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==1197==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000004cc (pc 0x0000006
==1197==The signal is caused by a READ memory access.
==1197==Hint: address points to the zero page.
    #0 0x6badae  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6badae)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f62e925ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==1197==ABORTING
```

sample file :

https://drive.google.com/file/d/1PXlJGUbUZxReuOTEuF8Pvny5hjNtXzJI/view?usp=sharing

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2966==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000036 (pc 0x0000004
==2966==The signal is caused by a READ memory access.
==2966==Hint: address points to the zero page.
    #0 0x4fbbb6  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbbb6)
    #1 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #2 0x7f3e141cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #3 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==2966==ABORTING
```

sample file :

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

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3991==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000036 (pc 0x0000004
==3991==The signal is caused by a READ memory access.
==3991==Hint: address points to the zero page.
    #0 0x4fe954  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe954)
    #1 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #2 0x7fee2bb48c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #3 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==3991==ABORTING
```

sample file :

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

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==8370==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000704 (pc 0x0000006
==8370==The signal is caused by a READ memory access.
==8370==Hint: address points to the zero page.
    #0 0x6babea  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6babea)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f8358612c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==8370==ABORTING
```

sample file :

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

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==9840==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000006
==9840==The signal is caused by a READ memory access.
==9840==Hint: address points to the zero page.
    #0 0x6b6a8f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6a8f)
    #1 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f4071149c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==9840==ABORTING
```

sample file :

https://drive.google.com/file/d/1QYTVBayBwZvLdp4VNkIxB696V8jmnxU6/view?usp=sharing

crash info

gradle

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==1585==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x000000703969 bp 0x7ffd
==1585==The signal is caused by a READ memory access.
==1585==Hint: this fault was caused by a dereference of a high value address (see reg
    #0 0x703969  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x703969)
    #1 0x65be5b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65be5b)
    #2 0x4fe2f1  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe2f1)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f72f8d40c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==1585==ABORTING
```

sample file :

https://drive.google.com/file/d/1v5-qJeZpmw7_txAnhI8ew82NW2BCdLFH/view?usp=sharing

crash info

gradle

```
=================================================================
==1985==ERROR: AddressSanitizer: SEGV on unknown address 0x61b000010076 (pc 0x0000006
==1985==The signal is caused by a READ memory access.
    #0 0x65f724  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65f724)
    #1 0x4fe89d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f4881d74c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0
==1985==ABORTING
```

received CVE id

CVE-2022-33047

Vulnerability type

use-after-free

sample file :

https://drive.google.com/file/d/1g3MQajVLZAaZMRflQHSLT6XRw-B4Dmz8/view?usp=sharing

command to reproduce:

shell

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

crash info

shell

```
==49487==ERROR: AddressSanitizer: heap-use-after-free on address 0x603000000011 at pc
READ of size 1 at 0x603000000011 thread T0
    #0 0x44cfbe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x44cfbe)
    #1 0x44e7dd in vsnprintf (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4
    #2 0x72a75e  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x72a75e)
    #3 0x72afc2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x72afc2)
    #4 0x4f65ac  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4f65ac)
    #5 0x7f6e50b86c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x41c549)

0x603000000011 is located 1 bytes inside of 20-byte region [0x603000000010,0x60300000
freed by thread T0 here:
```

```
    #0 0x4ae7d2 in free (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4ae7d2
    #1 0x4f5cf4  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4f5cf4)
    #2 0x7f6e50b86c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/

previously allocated by thread T0 here:
    #0 0x4aeb10 in malloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x4aeb
    #1 0x724f05  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccbuild+0x724f05)

SUMMARY: AddressSanitizer: heap-use-after-free (/home/bupt/Desktop/otfcc/bin/release-
Shadow bytes around the buggy address:
  0x0c067fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c067fff8000: fa fa[fd]fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8010: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
  0x0c067fff8020: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff8030: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fa fa
  0x0c067fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==49487==ABORTING
```

Author: Victory+

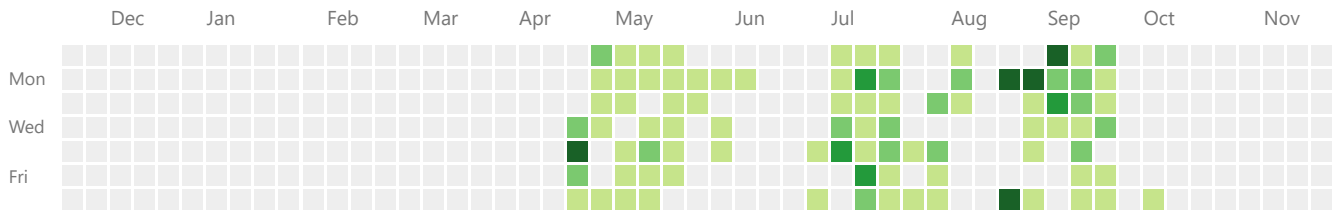
Link: https://cvjark.github.io/2022/07/06/CVE-2022-33047/

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

CVE

©2022 By Victory+

Victory+ ♥ TBaozi



Local search

Search for Posts

Powered by hexo-generator-search