Description

Tcache checks for double free by key since libc2.29.
To solve this problem, double-free tcache by overwriting the key

1. checksec

   Arch: amd64-64-little
   RELRO: Full RELRO
   Stack: Canary found
   NX: NX enabled
   PIE: PIE enabled
   FORTIFY: Enabled

2. Menu

- Buy ticket: malloc(0x18), (maximum 7 times to prevent using fastbins) (bof)
- View ticket: print malloced memory (leak libc) (array index check x)
- Use ticket: (without nullify address)

  one-time: free

  5 times pass: unused_count-=1 or free if unused_count==0

- Exit

3. Structure

one time ticket

```
0x00 |  first name   |    last name  |    onetime: one ride ticket(1), one day pass(0)
0x10 | ticket_type   |``````````````````````|
```

5 times pass

```
0x00 |  first name   |   last name  |
0x10 |  ticket_type  | meal |safari|
0x20 |  gift  |          |       ride      |
```

4. Exploit

1) view: leak libc address with negative array index(got)

3) malloc(0:onetime), malloc(1), malloc(2) -> free(2), free(1), free(0) -> malloc(0:onetime) -> overwrite onetime with terminating "\x00"

4) use(0) -> 2nd ticket's tcache_entry.key is changed

5) free(1) -> double free

6) malloc(1) -> overwrite tcache_entry.next with free hook or what ever

7) malloc(1: /bin/sh), malloc(free_hook) ->write system

8) free