

# 1. 修复内核模块

- 对 UAF 漏洞进行修复，操作即在 kfree 之后，添加对于指针的置空操作；
- 对空指针引用漏洞进行修复，操作即在使用指针之前判断该指针是否为空：

```
1 static int drill_act_exec(long act) {
2     int ret = 0;
3
4     switch (act) {
5         case DRILL_ACT_ALLOC:
6             ...
7
8         case DRILL_ACT_CALLBACK:
9             pr_notice("drill: exec callback %lx for item %lx\n",
10                      (unsigned long)drill.item->callback,
11                      (unsigned long)drill.item);
12             if (drill.item) {
13                 drill.item->callback(); // Add check by XBA, GOOD GOOD GOOD
14             }
15             // drill.item->callback(); // No check, BAD BAD BAD
16             break;
17
18         case DRILL_ACT_FREE:
19             pr_notice("drill: free item at %lx\n",
20                      (unsigned long)drill.item);
21             kfree(drill.item);
22             drill.item = NULL; // Add by XBA
23             pr_notice("drill: set item ptr to NULL\n"); // Add by XBA
24             break;
25
26         case DRILL_ACT_RESET:
27             ...
28
29         default:
30             ...
31     }
32
33     return ret;
34 }
```

## 2. 开启 SMAP

- 开启防御措施 SMAP (Supervisor Mode Access Prevention) 来禁止从内核空间访问用户空间:

```
1 # 使用该命令启动QEMU虚拟机, 使用-cpu kvm64, smap开启 smap
2 qemu-system-x86_64 \
3 -cpu kvm64, smap \
4 -kernel linux-5.0-rc1/arch/x86/boot/bzImage \
5 -append "console=ttyS0 root=/dev/sda debug earlyprintk=serial slub_debug=QUZ
6 -hda wheezy.img \
7 -net user, hostfwd=tcp::10021-:22 -net nic \
8 -nographic -m 512M -smp 2 \
9 -pidfile vm.pid 2>&1 | tee vm.log
```

- 开启 SMAP 后使用 drill\_exploit\_uaf 进行攻击失败：

```
Activities Terminal May 20 22:07
xubiang@ubuntu: ~/Desktop/NADP3/EXP5

[ 108.159428] ? vfs_write+0xa4/0x1a0
[ 108.160370] ? ksys_write+0x4e/0xb0
[ 108.161308] ? do_syscall_64+0x47/0xf0
[ 108.162495] ? entry_SYSCALL_64_after_hwframe+0x44/0xa9
[ 108.164025] Modules linked in: drill_mod(0)
[ 108.165693] Dumping ftrace buffer:
[ 108.166854] (ftrace buffer empty)
[ 108.168276] CR2: 00000000006012e8
[ 108.170334] ---[ end trace ce4e917fa938d1c1 ]---
[ 108.171644] RIP: 0010:0x40099e
[ 108.172474] Code: 55 bf 50 10 60 00 48 89 e5 ff d0 5d e9 7b ff ff ff e9 76 ff ff ff 90 90 55 48 89 e5 53 48 83 ec 18 48 89 7d e8
[ 108.177442] RSP: 0018:ffff9f6600477dc8 EFLAGS: 00000292
[ 108.178870] RAX: 000000001f215418 RBX: 0000000000000001 RCX: 0000000000000000
[ 108.180763] RDY: 0000000000000000 RSI: ffff99541f215418 RDI: ffff99541f215418
[ 108.182703] RBP: ffff9f6600477de8 R08: 00000000000001ef R09: 0000000000000044
[ 108.184945] R10: 632063657865203a R11: 206b6361626c6c61 R12: ffff99541bbb5458
[ 108.186929] R13: 00007fff82f59e18 R14: 0000000000000001 R15: ffff9f6600477f08
[ 108.188804] FS: 00007f5112a78700(0000) GS:ffff99541f200000(0000) knlGS:0000000000000000
[ 108.191038] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 108.192567] CR2: 00000000006012e8 CR3: 000000001885c000 CR4: 0000000002006f0
[ 108.194714] Kernel panic - not syncing: Fatal exception
[ 108.197058] Dumping ftrace buffer:
[ 108.198100] (ftrace buffer empty)
[ 108.199106] Kernel Offset: 0x10e00000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 108.202980] ---[ end Kernel panic - not syncing: Fatal exception ]---

drill@syzkaller:~$ ./drill_exploit_uaf
begin as: uid=1000, euid=1000
[+] payload:
      start at 0x7f5112a7b000
      callback 40098c
setxattr returned -1
```

- 开启 SMAP 后使用 `drill\_exploit\_nullderef` 进行攻击失败:

```
Activities Terminal May 20 22:09
xubiang@ubuntu: ~/Desktop/NADP3/EXP5

[ 113.226504] RIP: 0010:drill_act_write.cold+0x9b/0xd5 [drill_mod]
[ 113.228181] Code: eb af e8 03 7b ba fa 48 c7 c7 e0 0b c0 e8 d4 a2 bf fa 48 c7 c0 f2 ff ff ff eb 95 48 8b 15 ff 21 00 00 48 c7
[ 113.234580] RSP: 0018:ffffa9a700697df8 EFLAGS: 00000246
[ 113.236776] RAX: 0000000000000002 RBX: 0000000000000001 RCX: 0000000000000000
[ 113.239787] RDX: 0000000000000000 RSI: 000000000000000a RDI: ffffffff00ba168
[ 113.242697] RBP: 0000000000000001 R08: 0000000000000002 R09: 0000000000000001
[ 113.248804] R10: 000000000000000a R11: f000000000000000 R12: ffff93e9d9bb4a008
[ 113.254419] R13: 00007ffe5f57dfa8 R14: 0000000000000001 R15: fffffa9a700697f08
[ 113.259591] FS: 00007fa15fd21700(0000) GS:ffff93e9df300000(0000) knlGS:0000000000000000
[ 113.264245] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 113.266656] CR2: 0000000000000008 CR3: 000000001adce000 CR4: 0000000002006e0
[ 113.271437] Kernel panic - not syncing: Fatal exception
[ 113.278047] Dumping ftrace buffer:
[ 113.279466] (ftrace buffer empty)
[ 113.281113] Kernel Offset: 0x39c00000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 113.284568] ---[ end Kernel panic - not syncing: Fatal exception ]---

drill@syzkaller: ~$ ./drill_exploit_nullderef
[+] begin as: uid=1000, euid=1000
[+] mmap done
[+] open mem done
[+] addr:
10000 -> f000 -> e000 -> d000 -> c000 -> b000 -> a000 -> 9000 -> 8000 -> 7000 -> 6000 -> 5000 -> 4000 -> 3000 -> 2000 -> 1000 -> 0
[+] /proc/$PPID/maps:
00000000-00011000 rw-p 00000000 00:00 0
[+] data at NULL: 0x706f2064696c6156
[+] open drill done
[+] drill alloc done
[+] drill reset done
[+] payload:
    start at (nil)
    callback 4009ac
```