IntelFBClientControl 驱动审计笔记

Brightiup

2018 年 3 月 28 日

目录

1　驱动结构

2 安全问题

2.1 AppleIntelAzulController::SetFbStatusOnNextProbe 函数空指针解引用

ProductName	Mac OS X
ProductVersion	10.13.3
BuildVersion	17D102

```
__ZN24AppleIntelAzulController22SetFbStatusOnNextProbeEP14AGDCFBOnline_t:
0000000000039eea    movq    %rsi, %rax
0000000000039eed    incq    0x3b7b4(%rip)
0000000000039ef4    movl    (%rax), %ecx
0000000000039ef6    incq    0x3b52b(%rip)
0000000000039efd    movzbl  0xf5e(%rdi), %edx
0000000000039f04    cmpl    %ecx, %edx
0000000000039f06    jbe 0x39f12
0000000000039f08    movq    0xf68(%rdi,%rcx,8), %rsi
0000000000039f10    jmp 0x39f1b
0000000000039f12    incq    0x3b517(%rip)
0000000000039f19    xorl    %esi, %esi    <——— XOR
0000000000039f1b    incq    0x3b686(%rip)
0000000000039f22    movq    0x3f70(%rsi), %rcx <——— NULL Pointer
0000000000039f29    testb   $0x10, 0xc4(%rcx)
0000000000039f30    jne 0x39f53
0000000000039f32    movb    0x4(%rax), %al
...
0000000000039f7e    xorl    %eax, %eax
0000000000039f80    retq
0000000000039f81    nop
```

在 0x701 号函数 AppleIntelAzulController::SetFbStatusOnNextProbe 中 0x0000000000039f19 处置空后并没有返回,而是在 0x0000000000039f22 处继续引用。PoC:

```
*(uint32_t*)(structure_input + 0) = 0xffffffff;
```

2.2 AppleIntelAzulController::ConfigureAudio 函数空指针解引用

ProductName	Mac OS X
ProductVersion	10.13.3
BuildVersion	17D102

```
__ZN24AppleIntelAzulController14ConfigureAudioEP20AGDCAudioAssociate_t:
000000000003b4fe    pushq   %rbp
000000000003b4ff    movq    %rsp, %rbp
000000000003b502    pushq   %rbx
000000000003b503    pushq   %rax
000000000003b504    incq    0x3a5a5(%rip)
000000000003b50b    movl    (%rsi), %eax
000000000003b50d    incq    0x39f14(%rip)
000000000003b514    movzbl  0xf5e(%rdi), %ecx
000000000003b51b    cmpl    %eax, %ecx
000000000003b51d    jbe 0x3b529
000000000003b51f    movq    0xf68(%rdi,%rax,8), %rbx
000000000003b527    jmp 0x3b532
000000000003b529    incq    0x39f00(%rip)
000000000003b530    xorl    %ebx, %ebx       <---  XOR
000000000003b532    movb    $0x1, 0x2440(%rbx) <--- NULL Pointer
000000000003b539    movl    0x8(%rsi), %esi
...
000000000003b5d6    addq    $0x8, %rsp
000000000003b5da    popq    %rbx
000000000003b5db    popq    %rbp
000000000003b5dc    retq
000000000003b5dd    nop
```

在 0x926 号函数 AppleIntelAzulController::ConfigureAudio 中 0x000000000003b530 处对指针置空，在 0x000000000003b532 处又有引用。PoC:

```
*(uint32_t*)(structure_input + 0) = 0xffffffff;
```