TALOS VULNERABILITY REPORT

TALOS-2016-0088

APPLE OS X GEN6ACCELERATOR IOGEN575SHARED::NEW_TEXTURE LOCAL PRIVILEGE ESCALATION VULNERABILITY

MARCH 22, 2016

REPORT ID

CVE-2016-1743

SUMMARY

A vulnerability exists in the communication functionality of the Apple Intel HD 3000 Graphics kernel driver. A specially crafted message can cause a vulnerability resulting in local privilege escalation.

TESTED VERSIONS

Apple OSX Intel HD 3000 Graphics driver 10.0.0 - com.apple.driver.AppleIntelHD3000Graphics (10.0.0) D3CFD566-1AE5-3315-B91B-B8264A621EB5 <78 12 7 5 4 3 1>

PRODUCT URLS

http://apple.com

CVSSV3 SCORE

8.8 - CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C

DETAILS

This vulnerability can be triggered by sending specially crafted IOConnectCallMethod request to the AppleIntelHD3000Graphics driver.

Faulting code is located in the AppleIntelHD3000Graphics driver in the IOGen575Shared::new_texture function.

```
__text:000000000001AA17 loc_1AA17:                              ; CODE XREF: IOGen575Share
d::new_texture(ulong long,ulong long,ulong long,ulong long,uint,ulong long
*,ulong long *)+5Fj
__text:000000000001AA17                 mov     r14, cs:off_560B0
__text:000000000001AA1E                 mov     rbx, [r14]
__text:000000000001AA21                 add     r13, rax
__text:000000000001AA24                 lea     rax, [rbx+r13+3]
__text:000000000001AA29                 neg     rbx
__text:000000000001AA2C                 and     rbx, rax
__text:000000000001AA2F                 mov     rdi, [rdx+18h]          ; rdx=0 (null poin
ter - data from null page)
__text:000000000001AA33                 mov     r13, rdx
__text:000000000001AA36                 mov     eax, [rdi+1AB0h]        ; attacker control
 eax now
__text:000000000001AA3C                 mov     rcx, cs:off_560A8
__text:000000000001AA43                 mov     cl, [rcx]
__text:000000000001AA45                 shl     eax, cl
__text:000000000001AA47                 lea     rcx, _kLargeCommandSizeMin
__text:000000000001AA4E                 mov     ecx, [rcx]
__text:000000000001AA50                 add     ecx, ecx
__text:000000000001AA52                 sub     eax, ecx
__text:000000000001AA54                 cmp     rbx, rax
__text:000000000001AA57                 ja      loc_1AC8C               ; by forging rax a
ttacker can skip this jump
__text:000000000001AA5D                 mov     [rbp+var_54], esi
__text:000000000001AA60                 mov     rax, [rdi]
__text:000000000001AA63                 mov     esi, 168h
__text:000000000001AA68                 call    qword ptr [rax+980h]    ; this leads to co
de execution (pointer controlled by attacker)
```

The vulnerability is caused by instruction at address 0x1AA2F which references memory that is currently not available since RDX register points to zero. This vulnerability can lead to local privilege escalation since NULL page can be allocated on OSX systems. Attacker can forge the input data and force the system to execute instruction at 0x1AA68 which is a call pointer instruction. Where pointer data is completely controlled by attacker.

We have successfully exploited this vulnerability on OS X 10.11.

CRASH INFORMATION

```
Anonymous UUID:       47360100-9DC8-8EA0-F879-F28691AC90F1


Mon Nov  9 14:04:20 2015


*** Panic Report ***
panic(cpu 3 caller 0xffffff80063d6bba): Kernel trap at 0xffffff7f889e3a2f, type 14=page fa
ult, registers:
CR0: 0x0000000080010033, CR2: 0x0000000000000018, CR3: 0x0000000105adc027, CR4: 0x00000000
000626e0
RAX: 0x00000000cccce9f7, RBX: 0x00000000cccce000, RCX: 0x0000000000000088, RDX: 0x00000000
00000000
RSP: 0xffffff90b2d53aa0, RBP: 0xffffff90b2d53b00, RSI: 0x0000000000000008, RDI: 0x00000000
00000000
R8:  0x0000000000000000, R9:  0x00000000cccccccc, R10: 0xffffff90b2d53ba8, R11: 0xffffff80
16f0c600
R12: 0xffffff8011adeabc, R13: 0x00000000ccccd9f4, R14: 0xffffff8006a2c8a0, R15: 0x00000000
00000000
RFL: 0x0000000000010206, RIP: 0xffffff7f889e3a2f, CS:  0x0000000000000008, SS:  0x00000000
00000010
Fault CR2: 0x0000000000000018, Error code: 0x0000000000000000, Fault CPU: 0x3, PL: 0


Backtrace (CPU 3), Frame : Return Address
0xffffff90b2d53730 : 0xffffff80062e5307
0xffffff90b2d537b0 : 0xffffff80063d6bba
0xffffff90b2d53990 : 0xffffff80063f4313
0xffffff90b2d539b0 : 0xffffff7f889e3a2f
0xffffff90b2d53b00 : 0xffffff7f889e56a5
0xffffff90b2d53b50 : 0xffffff80068e3c82
0xffffff90b2d53b80 : 0xffffff80068e48fa
0xffffff90b2d53be0 : 0xffffff80068e1967
0xffffff90b2d53d20 : 0xffffff80063a07d0
0xffffff90b2d53e30 : 0xffffff80062e9aa3
0xffffff90b2d53e60 : 0xffffff80062cd478
0xffffff90b2d53ea0 : 0xffffff80062dcfd5
0xffffff90b2d53f10 : 0xffffff80063c13aa
0xffffff90b2d53fb0 : 0xffffff80063f4b36
      Kernel Extensions in backtrace:
         com.apple.driver.AppleIntelHD3000Graphics(10.0)[D3CFD566-1AE5-3315-B91B-B8264A621
EB5]@0xffffff7f889c9000->0xffffff7f88a2ffff
            dependency: com.apple.iokit.IOPCIFamily(2.9)[8E5F549E-0055-3C0E-93F8-E872A048E
31B]@0xffffff7f86b2d000
            dependency: com.apple.iokit.IOGraphicsFamily(2.4.1)[48AC8EA9-BD3C-3FDC-908D-09
850215AA32]@0xffffff7f8763a000


BSD process name corresponding to current thread: poc1
Boot args: debug=0x1 -v

Mac OS version:
15B42

Kernel version:
Darwin Kernel Version 15.0.0: Sat Sep 19 15:53:46 PDT 2015; root:xnu-3247.10.11~1/RELEASE_
X86_64
Kernel UUID: AB5FC1B4-12E7-311E-8E6F-9023985D8C1D
Kernel slide:     0x0000000006000000
Kernel text base: 0xffffff8006200000
__HIB  text base: 0xffffff8006100000
System model name: Macmini5,1 (Mac-8ED6AF5B48C039E1)


System uptime in nanoseconds: 9096437189164
last loaded kext at 280430056831: com.apple.filesystems.msdosfs 1.10 (addr 0xffffff7f88ecf0
00, size 69632)
last unloaded kext at 342241286226: com.apple.filesystems.msdosfs   1.10 (addr 0xffffff7f88
ecf000, size 61440)
loaded kexts:
com.apple.driver.AudioAUUC   1.70
com.apple.driver.AppleHWSensor   1.9.5d0
com.apple.driver.ApplePlatformEnabler   2.5.1d0
com.apple.driver.AGPM   110.20.21
com.apple.driver.pmtelemetry   1
com.apple.iokit.IOUserEthernet   1.0.1
com.apple.iokit.IOBluetoothSerialManager   4.4.2f1
com.apple.Dont_Steal_Mac_OS_X   7.0.0
com.apple.filesystems.autofs   3.0
com.apple.driver.AppleOSXWatchdog   1
com.apple.driver.AppleMikeyHIDDriver   124
com.apple.driver.AppleHDA   272.50.31
com.apple.driver.AppleUpstreamUserClient   3.6.1
com.apple.driver.AppleMCCSControl   1.2.13
com.apple.driver.AppleMikeyDriver   272.50.31
com.apple.driver.AppleIntelHD3000Graphics   10.0.0
com.apple.driver.AppleHV   1
com.apple.driver.AppleThunderboltIP 3.0.8
com.apple.iokit.BroadcomBluetoothHostControllerUSBTransport 4.4.2f1
com.apple.driver.AppleSMCPDRC   1.0.0
com.apple.driver.AppleLPC   3.1
com.apple.driver.AppleIntelSlowAdaptiveClocking 4.0.0
com.apple.driver.ACPI_SMC_PlatformPlugin   1.0.0
com.apple.driver.AppleIntelSNBGraphicsFB   10.0.0
com.apple.driver.AppleIRController   327.5
com.apple.AppleFSCompression.AppleFSCompressionTypeDataless 1.0.0d1
com.apple.AppleFSCompression.AppleFSCompressionTypeZlib 1.0.0
com.apple.BootCache 37
com.apple.iokit.IOAHCIBlockStorage   2.8.0
com.apple.driver.AppleFWOHCI   5.5.2
com.apple.driver.AirPort.Brcm4331   800.20.24
com.apple.driver.AppleSDXC   1.7.0
com.apple.iokit.AppleBCM5701Ethernet   10.1.11
com.apple.driver.usb.AppleUSBEHCIPCI   1.0.1
com.apple.driver.AppleAHCIPort   3.1.5
com.apple.driver.AppleACPIButtons   4.0
com.apple.driver.AppleRTC   2.0
com.apple.driver.AppleHPET   1.8
com.apple.driver.AppleSMBIOS   2.1
com.apple.driver.AppleACPIEC   4.0
com.apple.driver.AppleAPIC   1.7
com.apple.driver.AppleIntelCPUPowerManagementClient 218.0.0
com.apple.nke.applicationfirewall   163
com.apple.security.quarantine   3
com.apple.security.TMSafetyNet   8
com.apple.driver.AppleIntelCPUPowerManagement   218.0.0
com.apple.AppleGraphicsDeviceControl   3.11.33b1
com.apple.iokit.IOSurface   108.0.1
com.apple.iokit.IOSerialFamily   11
com.apple.kext.triggers 1.0
com.apple.driver.DspFuncLib 272.50.31
com.apple.kext.OSvKernDSPLib   525
com.apple.driver.CoreCaptureResponder   1
com.apple.driver.AppleSMBusController   1.0.14d1
com.apple.iokit.IOBluetoothHostControllerUSBTransport   4.4.2f1
com.apple.iokit.IOBluetoothFamily   4.4.2f1
com.apple.driver.AppleSMBusPCI   1.0.14d1
com.apple.iokit.IOFireWireIP   2.2.6
com.apple.driver.AppleHDAController 272.50.31
com.apple.iokit.IOHDAFamily 272.50.31
com.apple.iokit.IOAudioFamily   204.1
com.apple.vecLib.kext   1.2.0
com.apple.iokit.IONDRVSupport   2.4.1
com.apple.iokit.IOSlowAdaptiveClockingFamily   1.0.0
com.apple.driver.AppleSMC   3.1.9
com.apple.driver.IOPlatformPluginLegacy 1.0.0
com.apple.driver.IOPlatformPluginFamily 6.0.0d7
com.apple.iokit.IOGraphicsFamily   2.4.1
com.apple.iokit.IOSCSIArchitectureModelFamily   3.7.7
com.apple.driver.usb.IOUSBHostHIDDevice 1.0.1
com.apple.iokit.IOUSBHIDDriver   900.4.1
com.apple.driver.usb.AppleUSBHostCompositeDevice   1.0.1
com.apple.driver.usb.AppleUSBHub   1.0.1
com.apple.driver.AppleThunderboltDPInAdapter   4.1.2
com.apple.driver.AppleThunderboltDPOutAdapter   4.1.2
com.apple.driver.AppleThunderboltDPAdapterFamily   4.1.2
com.apple.driver.AppleThunderboltPCIDownAdapter 2.0.2
com.apple.driver.AppleThunderboltNHI   4.0.4
com.apple.iokit.IOThunderboltFamily 5.0.6
com.apple.iokit.IOFireWireFamily   4.5.8
com.apple.iokit.IOEthernetAVBController 1.0.3b3
com.apple.iokit.IO80211Family   1101.24
com.apple.driver.mDNSOffloadUserClient   1.0.1b8
com.apple.iokit.IONetworkingFamily 3.2
com.apple.driver.corecapture   1.0.4
com.apple.iokit.IOAHCIFamily   2.8.0
com.apple.driver.usb.AppleUSBEHCI   1.0.1
com.apple.iokit.IOUSBFamily 900.4.1
com.apple.iokit.IOUSBHostFamily 1.0.1
com.apple.driver.AppleUSBHostMergeProperties   1.0.1
com.apple.driver.AppleEFINVRAM   2.0
com.apple.driver.AppleEFIRuntime   2.0
com.apple.iokit.IOHIDFamily 2.0.0
com.apple.iokit.IOSMBusFamily   1.1
com.apple.security.sandbox   300.0
com.apple.kext.AppleMatch   1.0.0d1
com.apple.driver.AppleKeyStore   2
com.apple.driver.AppleMobileFileIntegrity   1.0.5
com.apple.driver.AppleCredentialManager 1.0
com.apple.driver.DiskImages 415
com.apple.iokit.IOStorageFamily 2.1
com.apple.iokit.IOReportFamily   31
com.apple.driver.AppleFDEKeyStore   28.30
com.apple.driver.AppleACPIPlatform   4.0
com.apple.iokit.IOPCIFamily 2.9
com.apple.iokit.IOACPIFamily   1.4
com.apple.kec.Libm   1
com.apple.kec.pthread   1
com.apple.kec.corecrypto   1.0
```

CREDIT

Discovered by Piotr Bania of Cisco Talos.

TIMELINE

2016-02-02 - Vendor Disclosure

2016-03-22 - Public Release