**Compiled by Le Cao Nguyen (**[**nguyenlc1993@gmail.com**](mailto:nguyenlc1993@gmail.com)**)**

**Summary of AppleUSBXHCI patches**

**A. How to disassemble AppleUSBXHCI driver**

1. Install Xcode

2. Run this command (doesn’t require root privilege):

otool -tv /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/AppleUSBXHCI.kext/Contents/MacOS/AppleUSBXHCI > ~/Desktop/AppleUSBXHCI.dsm.txt

Output of otool will be flushed to AppleUSBXHCI.dsm.txt on desktop.

**B. List of patches**

These patches are applied only on AppleUSBXHCI version 705.4.14 (Mac OS X 10.10). Newer versions may require these patches to be updated.

1. Disable Intel & Fresco Logic USB3.0 controllers check (to allow non-Intel USB3 controllers):

Module: *\_\_ZN12AppleUSBXHCI13UIMInitializeEP9IOService*

Offset: *0x12086*

Format: j*ne 0x1\*\*\*\**

Evidence: *testb $-0x80, 0xd4(%rax)* **line above**

Patch: *jne* to *jmp*

Binary patch: 80 D4 00 00 00 80 75 34

80 D4 00 00 00 80 **EB** 34

or just 00 80 75 34

00 80 **EB** 34

2. Disable XHCI 1.0 check (to allow older XHCI version, such as 0.96 of Renesas/NEC controller):

Module: *\_\_ZN12AppleUSBXHCI13UIMInitializeEP9IOService*

Offset: *0x12160*

Format: *cmpl $0x100, %eax*

Evidence: *movl $0xe00002c7, %r12d ## imm = 0xE00002C7* **line above**

Patch: *100* to *000*

Binary patch: 3D 00 01 00 00 0F 82 7A

3D 00 **00** 00 00 0F 82 7A

or just E0 3D 00 01

E0 3D 00 **00**

3. Patch MSI or pin interrupts:

Module: *\_\_ZN12AppleUSBXHCI13AddressDeviceEjtbhii*

Offset: *0x144a3*

Format: *orl $0x400000, 0x8(%rcx) ## imm = 0x400000*

Patch: *400000* to *000000*

Binary patch: 81 49 08 00 00 40 00 41

81 49 08 00 00 **00** 00 41

Module: *\_\_ZN12AppleUSBXHCI15\_createTransferEPvbyjybbPjS1\_bPs*

Offset: *0x1574c*

Format: *movl $0x400000, 0x8(%r15) ## imm = 0x400000*

Patch: *400000* to *000000*

Binary patch: 41 C7 47 08 00 00 40 00

41 C7 47 08 00 00 **00** 00

Module: *\_\_ZN12AppleUSBXHCI15\_createTransferEPvbyjybbPjS1\_bPs*

Offset: *0x159bc*

Format: *movl $0x400000, 0x8(%r15) ## imm = 0x400000*

Patch: *400000* to *000000*

Binary patch: 41 C7 47 08 00 00 40 00

41 C7 47 08 00 00 **00** 00

Binary patch for 3 sub-patches: 08 00 00 40

08 00 00 **00**

4. Disable the sleep code leaving the controller in non-working state after wake (IOUSBFamily will turn off the controller and restart it after wake):

Module: *\_\_ZN12AppleUSBXHCI20CheckSleepCapabilityEv*

Offset: *0x643e*

Format: *movb $0x1, 0xc8(%rax)*

Evidence: *movq 0xa8(%rbx), %rax* **line above**

Patch: *0x1* to *0x0*

Binary patch: C6 80 C8 00 00 00 01 48

C6 80 C8 00 00 00 **00** 48

or just C8 00 00 00 01 48

C8 00 00 00 **00** 48

5. Enable PCI power management (if there is no such code in DSDT):

Module: *\_\_ZN12AppleUSBXHCI20CheckSleepCapabilityEv*

Offset: *0x64a6*

Format: *jne 0x\*\*\*\**

Evidence: *testq %rax, %rax* **line above**

Patch: *jne* to *jmp*

Binary patch: 02 00 00 48 85 C0 75 4D

02 00 00 48 85 C0 **EB** 4D

or just 85 C0 75 4D

85 C0 **EB** 4D

**C. Sources**

<http://www.insanelymac.com/forum/topic/285157-patched-appleusbxhci-from-os-1082/>

<http://www.insanelymac.com/forum/files/file/150-patched-appleusbxhci/>