

macOS 11 BigSur Dev-Beta Clover Patch

Beitrag von „kuckkuck“ vom 2. Juli 2020, 17:32

Normalerweise bin ich hier ja nicht bekannt dafür mit Clover unterwegs zu sein. Trotzdem hier mal was für die Clover Gemeinde.

Ich habe in der Vergangenheit schon das ein oder andere mal KernelPatches verfasst, meistens im Bezug auf Ozmosis. Da ich mir mit dem Release von Big Sur wieder KextInjection Patches nach Clover/Ozmosis- (allgemein KernelBooterExtension-) Methode rausgeschrieben habe, dachte ich mir implementier ich sie doch einfach mal in Clover und schau ob Clover mit Big Sur umgehen kann. Ich habe ein paar Tests zusammen mit [CMMChris](#) unternommen und nach ein paar Versuchen war es möglich seine bestehende Installation von Big Sur zu booten.

Daraufhin habe ich mich daran versucht die nötigen Mechanismen in Clover einzubauen. Leider habe ich es bis zum jetzigen Zeitpunkt nicht schaffen können die internen Mechanismen, die mit Big Sur kaputt gegangen sind, wieder zum Leben zu erwecken. Da ich mich nie wirklich mit Clover, insbesondere Clover Source Code beschäftigt habe und letzterer leider mehr als unstrukturiert ist, fehlt mir hier der Durchblick um eine saubere und dauerhafte Lösung in Clover zu implementieren. Ich denke hier ist die Arbeit von langjährigen Clover Devs gefragt, die ihren eigenen Code kennen. Trotzdem will ich die Zwischenergebnisse hier mal veröffentlichen, damit andere darauf aufbauen können und jeder der will ein bisschen rumtesten kann.

Technischer Hintergrund:

Die Clover Version im Anhang setzt beim Boot von macOS Big Sur automatisch die NVRam Variablen `booter-fileset-kernel` und `booter-fileset-basesystem`, sodass beim Boot einer bestehenden Installation von Big Sur automatisch der prelinked kernel forciert wird. Der Boot eines Installers ist so nicht möglich, da kein passender prelinkedkernel existiert und auf diese Weise geladen werden kann. Selbst bei forciertem prelinkedkernel versagen leider Clovers interne KernelBooterExtension Patches, laut meinen Tests wird die Prozedur nicht gestartet da `OnExitBootServices` in den Tests wohl nicht eintritt. Beim forcieren des KernelPatches ohne Event wird der Kernel nicht gefunden. Was hingegen schon funktioniert sind User KernelPatches. Deswegen stelle ich die nötigen KernelBooterExtension-Patches für Big Sur als `KernelToPatch` Einträge bereit. Die Patches könnten bei Bedarf noch symbolbasiert implementiert werden. In der angehängten Clover Version sind die eigentlichen internen Patchingmechanismen für den Boot von Big Sur (10.16) deaktiviert um Dopplungen zu meiden.

Alle Patches suchen nach dem Anfang des entsprechenden Procedures und danach nach der passenden Patching Location. Ebenfalls sind alle Patches mit einfachen Wildcards implementiert.

KbeBS-EXT sucht nach readStartupExtensions (010031FFBE140005), der Patch lautet:

```
E8 ?? 00 00 00 EB 05 E8 -->
```

```
E8 ?? 00 00 00 90 90 E8.
```

KbeBS-SIP sucht nach loadExecutable (02000041BF010000DC), der Patch lautet:

```
E8 ?? ?? ?? 00 85 C0 0F 84 ?? 00 00 00 49 8B 45 -->
```

```
E8 ?? ?? ?? 00 85 C0 90 90 90 90 90 90 49 8B 45.
```

KbeBS-KxldUnmap sucht nach removeKextBootstrap (488D152B262500), der Patch lautet:

```
FF 80 3D ?? ?? ?? 00 00 0F 85 ?? 01 00 00 41 -->
```

```
FF 80 3D ?? ?? ?? 00 00 90 E9 ?? 01 00 00 41.
```

Veränderungen und Plist für macOS Big Sur BETA 3+: [KernelToPatch Einträge BETA 3](#)

Beta 3

Des Weiteren ist die Nutzung von OCQuirks zwingende Voraussetzung zum Boot von Big Sur, da jegliche alte AptioFix Varianten nicht kompatibel sind. In dem [neuesten OCQuirks Release](#) sind Änderungen zu [AvoidRuntimeDefrag](#) enthalten, ohne die der Boot von macOS Big Sur 10.16/11 nicht möglich ist.

Benutzung:

- CLOVERX64.efi (r5119 Mod) auf der EFI durch den Anhang ersetzen
- Folgende KernelToPatch Einträge in die config.plist einfügen: (Wer nicht weiß wie das geht ist fehl am Platz - sorry)

Code

1. <key>KernelAndKextPatches</key>
2. <dict>
3. <key>KernelToPatch</key>
4. <array>
5. <dict>

6. <key>Comment</key>
7. <string>KbeBS-EXT (kuckkuck)</string>
8. <key>Count</key>
9. <integer>1</integer>
10. <key>Disabled</key>
11. <false/>
12. <key>Find</key>
13. <data>
14. 6NQAAADrBeg=
15. </data>
16. <key>MaskFind</key>
17. <data>
18. /wD////////8=
19. </data>
20. <key>MaskReplace</key>
21. <data>
22. AAAAAAD///8=
23. </data>
24. <key>MatchOS</key>
25. <string>10.16</string>
26. <key>Replace</key>
27. <data>
28. 6NQAAACQkOg=
29. </data>
30. <key>StartPattern</key>
31. <data>
32. AQAx/74UAAU=
33. </data>
34. </dict>
35. <dict>
36. <key>Comment</key>
37. <string>KbeBS-SIP (kuckkuck)</string>
38. <key>Count</key>
39. <integer>1</integer>
40. <key>Disabled</key>
41. <false/>
42. <key>Find</key>
43. <data>
44. 6HXmDgCFwA+E+gAAAEMLRQ==
45. </data>
46. <key>MaskFind</key>
47. <data>


```
90. <key>StartPattern</key>
91. <data>
92. SI0VKyYIAA==
93. </data>
94. </dict>
95. </array>
96. </dict>
```

Alles anzeigen

- Jegliche benutzten OsxAptioFix.efi oder AptioMemoryFix.efi UEFI Treiber durch den neuesten [OCQuirks Release](#) ersetzen und OCQuirks.efi, OpenRuntime.efi und OcQuirks.plist nach /Clover/drivers/UEFI legen.
- Acidanthera Kexts durch [neu kompilierte Versionen](#) ersetzen, oder lilubetaall benutzen.

**Es können ausschließlich vorhandene Installationen von Big Sur gebootet werden.
Die Installation von Big Sur per Installer ist nicht möglich.**

Viel Spaß beim Testen und ansonsten mal Abwarten wann etwas von den Clover Entwicklern kommt.