macOS 11 BigSur Dev-Beta Clover Patch

Beitrag von „kuckkuck“ vom 24. Juli 2020, 21:21

Gemäß den besprochenen Veränderungen am Kernel von **macOS Big Sur BETA 3**:

1. OSVersion lautet mit Beta 3+ `11.0` und nicht mehr `10.16`. Die bisherigen Patches werden nur auf 10.16 angewandt. 11.0 muss also durch ein Komma getrennt zu MatchOS hinzugefügt werden.

2. Die Suche nach dem StartPattern (488D152B262500) für Kxld ist verändert, das StartPattern heißt jetzt 488D157C542500. Dieses Bytepattern wird sich in der Zukunft weiter verändern und die Suche wieder kaputt gehen!
Einfacher Fix:

Code

1. <key>StartPattern</key>
2. <data>SI0VKyYlAA==</data>

komplett aus der Plist entfernen, der Patch ist auch so einmalig und somit unproblematisch, da er relativ präzise gewählt ist.

Alternativ die alten Werte durch das neue StartPattern ersetzen:

Code

1. <key>StartPattern</key>
2. <data>SI0VfFQlAA==</data>

Sinnvoller Fix: Symbolbasierte Suche mit procedure = removeKextBootstrap oder StartPattern mit Wildcards implementieren (`00 00 00 00 c7 45 ?? 00 00 00 00 48 8d 15`). Für Ersteres muss die MACH-O Bibliothek wieder funktionieren und für Letzteres muss die Suche nach StartPattern mit Wildcards möglich sein. Ich denke die offizielle Clover Version sollte bald auf diese Art und Weise funktionieren.

Allgemein: Es ist nicht eindeutig, ob der Kxld Patch unter Big Sur auf allen Systemen notwendig

ist, oder ob die dahinterliegende Race Condition garnicht erst entsteht. Eventuell kann der Fix also sogar ganz weg gelassen werden bzw. booten manche Systeme auch ohne Kxld Patch.

Eine mögliche Plist mit den KernelPatches für Beta 3 sieht also wie folgt aus:

Code

```
<key>KernelAndKextPatches</key>
<dict>
<key>KernelToPatch</key>
<array>
<dict>
<key>Comment</key>
<string>KbeBS-EXT (kuckkuck)</string>
<key>Count</key>
<integer>1</integer>
<key>Disabled</key>
<false/>
<key>Find</key>
<data>
6NQAAADrBeg=
</data>
<key>MaskFind</key>
<data>
/wD//////8=
</data>
<key>MaskReplace</key>
<data>
AAAAAAD//wA=
</data>
<key>MatchOS</key>
<string>10.16,11.0</string>
<key>Replace</key>
<data>
6NQAAACQkOg=
</data>
<key>StartPattern</key>
<data>
AQAx/74UAAU=
</data>
</dict>
<dict>
```

<key>Comment</key>
<string>KbeBS-SIP (kuckkuck)</string>
<key>Count</key>
<integer>1</integer>
<key>Disabled</key>
<false/>
<key>Find</key>
<data>
6EUEDwCFwA+E+gAAAEmLRQ==
</data>
<key>MaskFind</key>
<data>
/wAAAP//////AP//////w==
</data>
<key>MaskReplace</key>
<data>
AAAAAAAAAP//AAAAAAAAAA==
</data>
<key>MatchOS</key>
<string>10.16,11.0</string>
<key>Replace</key>
<data>
6EUEDwCFwOsE+gAAAEmLRQ==
</data>
<key>StartPattern</key>
<data>
AgAAQb8BAADc
</data>
</dict>
<dict>
<key>Comment</key>
<string>KbeBS-KxldUnmap (vit9696, kuckkuck)</string>
<key>Count</key>
<integer>1</integer>
<key>Disabled</key>
<false/>
<key>Find</key>
<data>
/4A9tcZOAAAPhRcBAABB
</data>
<key>MaskFind</key>
<data>

78. ////AAAA/////wD/////
79. </data>
80. <key>MaskReplace</key>
81. <data>
82. AAAAAAAAAAD//wAAAAAA
83. </data>
84. <key>MatchOS</key>
85. <string>10.16,11.0</string>
86. <key>Replace</key>
87. <data>
88. /4A9tcZOAACQ6RcBAABB
89. </data>
90. </dict>
91. </array>
92. </dict>

Alles anzeigen

StartPattern kann für KbeBS-KxldUnmap wieder hinzugefügt werden.