macOS 11 BigSur Dev-Beta Clover Patch

Beitrag von „kuckkuck“ vom 24. Juli 2020, 13:03

Die wichtigen KextInjection-Patches aus dem Eingangspost laufen auch noch mit Beta 3, bis auf `KbeBS-KxldUnmap`. Hierzu folgende Bemerkung im Eingangspost:

IMPORTANT: Beta 3

> Zitat von kuckkuck
>
> 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>
>
> unter KbeBS-KxldUnmap 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.
>
> 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 System auch ohne Kxld Patch.
>
> Alles anzeigen

Wer Big Sur Beta 3 mit Clover verwenden will, dem empfehle ich `StartPattern` aus dem `KbeBS-KxldUnmap` zu löschen.