Erledigt OpenCore Board-ID Skip und Spoof mit VMM Patch >> macOS Monterey plus Updates trotz nicht unterstützter Board-ID

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 22:55

TECHNIKVERBOT hat mich heute in diesem Thread darauf aufmerksam gemacht, dass die neuste Version des OpenCore Legacy Patches neue Booter und Kernel Patches enthält:

> Zitat
>
> Man könnte sich überlegen, den VMM Kernel Patch von parrotgeek1, der seit heute im Mainline Repository in OCLP angekommen ist, auf jedem Hackintosh mit unsupported SMBIOS reinzuklatschen. Damit würde man die Vorteile eines plattformgerechten SMBIOS inkl. Power Management und gleichzeitig nativen macOS Big Sur und Monterey Support durch das Vorgaukeln einer virtuellen Maschine beim Installer und SoftwareUpdateCore genießen.

Also habe ich das ganze getestet

Die Booter Patches gaukeln macOS via VMM eine unterstütze Board-ID vor, während die Hardware die unter PlatforInfo eingestellte verwendet. Und über diesen Umweg kann man dann SystemUpdates installieren trotz "falscher" Board-ID:

> Zitat
>
> Parrotgeek1's VMM patch set would force kern.hv_vmm_present to always return True. With hv_vmm_present returning True, both OSInstallerSetupInternal and SoftwareUpdateCore will set the VMM-x86_64 board ID while the rest of the OS will continue with the original ID.
>
> https://github.com/dortania/Op...Legacy-Patcher/issues/543

Das beste daran ist, dass man so ein SMBIOS, das zur verwendeten CPU passt und somit das CPU Power Management besser funktioniert – insbesondere bei Laptops.

Nützlich für CPUs folgender Familien:

- Sandy Bridge
- Ivy Bridge
- Haswell (partiell)

Hier ist die plist mit den Booter und Kernel Patches. Aktuell sind 3 der Kernel Patches aktiviert. Falls man eine Sandy Bridge CPU verwendet, benötigt man auch die restlichen (siehe Beschreibung): BoardIDSkip+VMMPatch_V2.plist

Weiteres Plus: falls eine Monterey beta Updates nicht angeboten werden, kann man das mit diesen Patches ebenfalls beheben.

Zu den Kernel Patches im EInzelnen:

- 0 bis 2: Aktivieren Board-ID Spoof via VMM unter macOS 12.0.1 (aktiv)
- Patch 3 scheint sich auf Apple Hardware zu beziehen (deaktiviert)
- Patch 4 deaktiviert Library Validation Enforcement. Mehr infos hier (thx atl)
- Patches 5-6: für Race Condition Fix bei Sandy Bridge und älter CPUs ab macOS 11.3, damals vor allem ein großes Problem beim MacPro5,1, wo neuere Big Sur Builds deswegen sehr selten booten konnten. (danke TECHNIKVERBOT)
- Patches 7-8: Experimentelle Patches um Sandy Bridge CPU support zu aktivieren (in macOS Monterey 12.1 beta rausgeflogen)

Zum Schluss noch FeatureUnlock.kext einbinden, um Content Caching zu aktivieren: https://github.com/acidanthera/FeatureUnlock

Viel Erfolg

Weitere Infos, für User, die macOS Monterey auf System älter als Ivy Bridge installieren wollen: https://forums.macrumors.com/t...-an-ongoing-saga.2320479/

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:03

wenn ich das also anhand der Patches und den Erklärungen von Khronokernel richtig verstehe:

- boot.efi Patch patcht lediglich den Board-ID Check raus

- die beiden Kernel Patches setzen die VM Präsenz wahr, sodass lediglich Installer und Software Update denken, es wäre eine virtuelle Maschine, dadurch, dass die CPU-ID aber nicht gespoofed wird bzw. da mitbetroffen ist, funktionieren Dinge wie natives Power Management und die korrekten Power Status dank Plattformzugehörigkeit beim SMBIOS einwandfrei.

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:04

Ja, so habe ich das auch verstanden. Eigentlich muss ich jetzt warten, bis ein Update kommt, um zu checken, ob's funzt.

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:08

> Zitat von 5T33Z0
>
> Ja, so habe ich das auch verstanden. Eigentlich muss ich jetzt warten, bis ein Update kommt, um zu checken, ob's funzt.

12.1 Beta ist heute dafür rausgekommen. XD

Und Apropo 12.1: Die haben jetzt ungelogen alle CPUs ohne RDNAND (also Sandy Bridge und älter) rausgeworfen!

macOS Monterey 12.1 Beta 1 (21C5021h) and RDRAND requirement · Issue #650 · dortania/OpenCore-Legacy-Patcher (github.com)

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:12

Okay. Wow, dann IvyBridge als nächstes. Ätzend

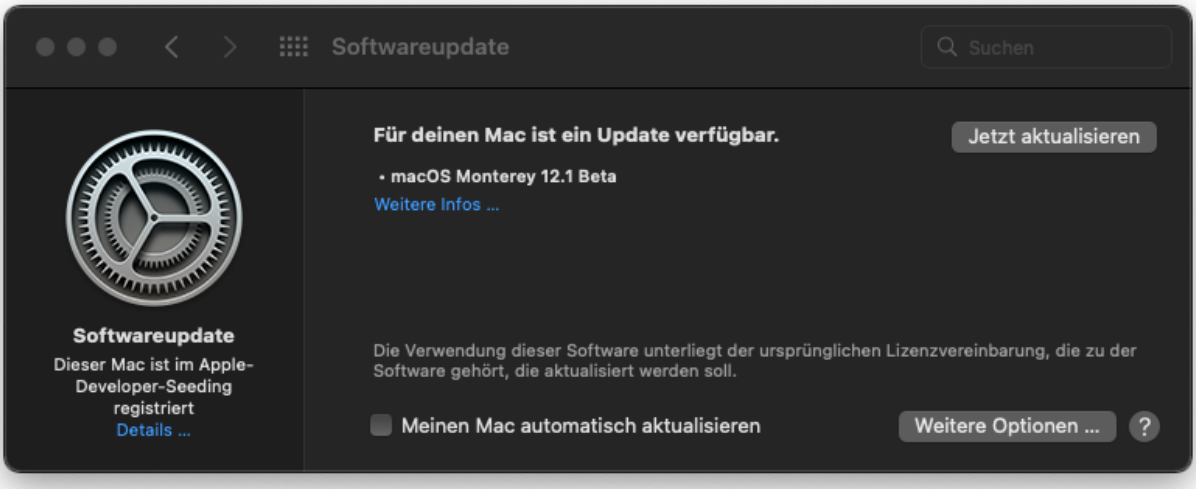
Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:13

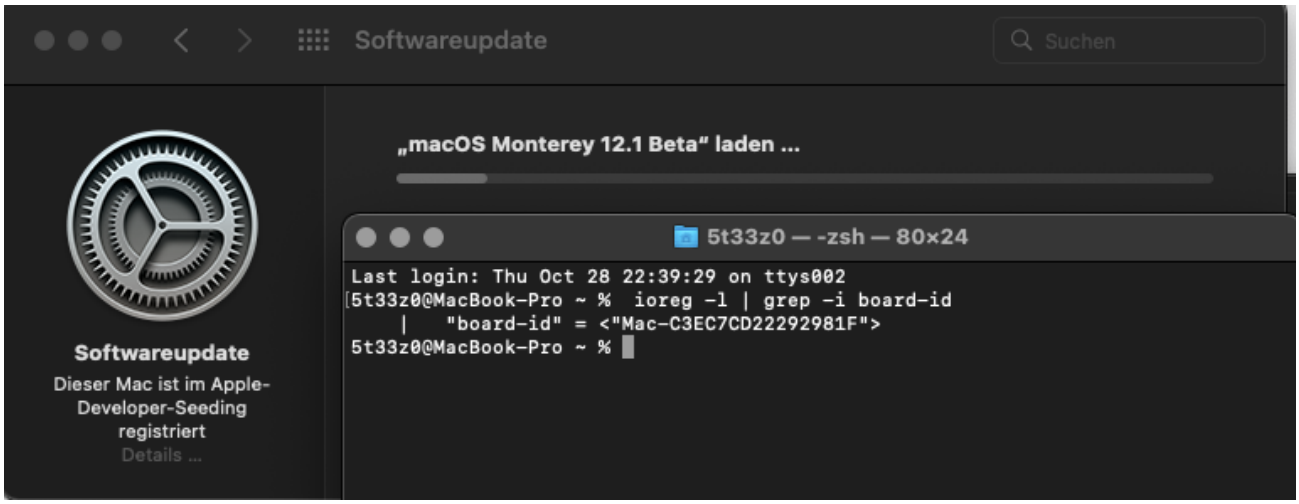
Wenigstens kein AVX2 😛

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:17

Boom! Update von macOS Monterey mit nicht unterstützer Board-ID

ES FUNKTIONIERT!!





Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:18

*insert "*click* NOICE" gif here*

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:19

Danke für den Tipp! Meeeeeeeega.

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:21

Gern. Hätte nicht gedacht, dass so eine zufällig spontane Idee von mir jetzt einfach so hilfreich wäre.

Einfach Patches für echte Macs kangen. XD

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:25

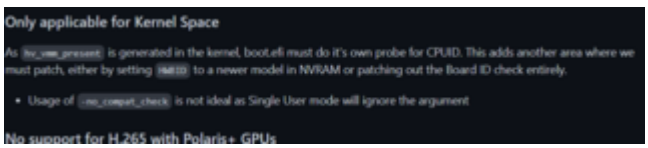
Was bedeutet der wohl? "Reroute HW_BID to OC_BID" HW= hardware, aber was ist BID?

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:26

BID = Board-ID schätze ich?

Oh

Supporting Spoofless Usage · Issue #543 · dortania/OpenCore-Legacy-Patcher (github.com)



Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:29

Also läuft die Kiste jetzt im SIngle User Mode, meinste?

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:30

ne, wenn man im Single-User Mode bootet, wird der -no_compat_check boot-arg ignoriert

---

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:32

Okay, Single User habe ich das letzte mal 2009 auf nem MacBookPro mit Intel Core Duo benutzt

---

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:33

da der Board-ID check wohl ja in Booter für's erste rausgepatched wurde, besteht denke ich für's erste auch kaum Handlungsbedarf.

Wird sich zeigen, ob macOS das 12.1 OTA-Update erfolgreich installieren will, oder auch nicht XD

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:36

Download läuft. Da ich Intel HD Patcher verwende, ist das seal broken und ich muss die kompletten 12 Gigs runterladen.

Beitrag von „TECHNIKVERBOT“ vom 28. Oktober 2021, 23:38

Schmerz... Kannte ich von meinem echten MacBookPro9,2 auf 12.0 Betas.

Beitrag von „5T33Z0“ vom 28. Oktober 2021, 23:51

Die Limitierung zweier Kernel patches auf MaxKernel 21.1.0 macht mir Sorgen. Denke das Beta update wir mindesten Kernel 21.2.0 sein.

Beitrag von „TECHNIKVERBOT“ vom 29. Oktober 2021, 09:29

Mir mal die Config.plist angesehen und kann sagen:

Kernel Patch 4 schaltet AMFI direkt über den XNU Kernel selbst ab, statt über amfi_get_out_of_my_way=0x1

5-6 sind Patches für den Race Condition Fix bei Sandy Bridge und älter CPUs ab macOS 11.3, damals vor allem ein großes Problem beim MacPro5,1, wo neuere Big Sur Builds deswegen sehr selten booten konnten.

Beitrag von „5T33Z0“ vom 29. Oktober 2021, 09:34

Danke. Weiß leider nicht, was AMFI und Race Condition bedeutet, aber füge es mal als Infos hinzu.

Beitrag von „atl“ vom 29. Oktober 2021, 09:48

5T33Z0, AMFI ist die Apple Mobile File Integrity, hier ganz gut beschrieben: https://www.naut.ca/blog/2020/...mmands-to-liberate-macos/

Beitrag von „TECHNIKVERBOT“ vom 29. Oktober 2021, 09:55

Kaum hab ich mich über Monterey 12.1 aufgeregt, schon existiert ein experimenteller Patch für die rdrand-Vorraussetzung:

Add Experimental 12.1 Beta 1 Patch · dortania/OpenCore-Legacy-Patcher@c6b3aaa

Beitrag von „schabulske“ vom 29. Oktober 2021, 09:59

5T33Z0

mal eine dumme Frage.

Würde das bedeuten das die HD4000 bei einem Update auf Monterey nicht gepatched werden muss?

Kann doch eigentlich nicht sein oder? da die Treiber aus Monterrey entfernt wurden oder habe ich jetzt einen Denkfehler 

Beitrag von „TECHNIKVERBOT“ vom 29. Oktober 2021, 10:02

> Zitat von schabulske
>
> Würde das bedeuten das die HD4000 bei einem Update auf Monterey nicht gepatched werden muss?

Nein, lediglich, dass OTA Updates und macOS Installationen nicht mehr aufgrund eines nicht unterstützten SMBIOS blockiert werden.

Beitrag von „5T33Z0“ vom 29. Oktober 2021, 10:03

> Zitat von schabulske
>
> 5T33Z0
>
> mal eine dumme Frage.
>
> Würde das bedeuten das die HD4000 bei einem Update auf Monterey nicht gepatched werden muss?
>
> Kann doch eigentlich nicht sein oder? da die Treiber aus Monterrey entfernt wurden oder habe ich jetzt einen Denkfehler
>
> Alles anzeigen

Patchen muss man weiterhin, weil die Treiber fehlen.

Beitrag von „schabulske“ vom 29. Oktober 2021, 10:07

TECHNIKVERBOT

5T33Z0

OK das heisst also weiterhin das man die SIP deaktivieren muss um die HD4000 Patches zu machen. Dann würde man aber wieder kein kleines Update via dem Updater angeboten bekommen und muss mit Fullinstaller drüber? Richtig?

Und dann wieder von vorne Patchen. Oder würde er trotzdem nur ein kleines Update machen und die Treiber bleiben erhalten indem man die SIP wieder vollständig aktiviert bzw geht das

überhaupt da ja eigentlich nach dem Patch der Seal Broken ist?

Fragen über Fragen? Sorry 

Beitrag von „5T33Z0“ vom 29. Oktober 2021, 10:09

Das hatte ich schon im Verlauf der Diskussion geschrieben: sobald man Treiber rein patcht ist das Siegel gebrochen und man muss immer den gesamten installer runterladen leider.

SIP kann man nicht aktivieren, wenn man Treiber reinpatcht, dann startet die Kiste nicht mehr.

Updates bekommt man angeboten. Sieht man ja in den Screenshots. Verwendeter Wert für csr-active-config in meinem Fall: 67080000

Beitrag von „TECHNIKVERBOT“ vom 29. Oktober 2021, 10:12

Genau, unter Software Update wirst du es zwar angezeigt bekommen, aber wegen dem gebrochenen Seal werden es keine Delta-Updates mehr, sondern full OTAs.

Beitrag von „schabulske“ vom 29. Oktober 2021, 10:14

Danke euch beiden fürs klarstellen 

Beitrag von „5T33Z0“ vom 29. Oktober 2021, 10:16

> Zitat von TECHNIKVERBOT
>
> Kaum hab ich mich über Monterey 12.1 aufgeregt, schon existiert ein experimenteller Patch für die rdrand-Vorraussetzung:
>
> Add Experimental 12.1 Beta 1 Patch · dortania/OpenCore-Legacy-Patcher@c6b3aaa

Baue ich dann später in die plist ein.

Beitrag von „TECHNIKVERBOT“ vom 15. November 2021, 08:13

Commits · acidanthera/FeatureUnlock (github.com)

HAHA, ja Moin

Beitrag von „5T33Z0“ vom 15. November 2021, 08:24

TECHNIKVERBOT:

Ah, danke für die Info. Scheint allerdings nicht das ganze Patch-Konstrukt zu sein, sondern sich nur auf Caching zu beziehen:

> Zitat
>
> # Content Caching Unlock
>
> For systems returning 1 from 'sysctl kern.hv_vmm_present'

Beitrag von „apfel-baum“ vom 15. November 2021, 08:36

liest sich ja interessant, und wenn ich richtig verstehe-kann es gut möglich sein, das der

support vom ivy "irgendwann" im laufe der updates von monterey selbst verschwindet = keine updates mehr? . wer weiß das wäre nun mutmaßung meinerseits

---

Beitrag von „GoodBye“ vom 22. November 2021, 23:19

> Zitat von 5T33Z0
>
> Das hatte ich schon im Verlauf der Diskussion geschrieben: sobald man Treiber rein patcht ist das Siegel gebrochen und man muss immer den gesamten installer runterladen leider.
>
> SIP kann man nicht aktivieren, wenn man Treiber reinpatcht, dann startet die Kiste nicht mehr.
>
> Updates bekommt man angeboten. Sieht man ja in den Screenshots. Verwendeter Wert für csr-active-config in meinem Fall: 67080000

Kann ja sein ich habe das nicht richtig verstanden, aber ich habe die Kepler Treiber in Monterey "rein gepatched" und danach wieder SIP aktiviert ohne Problem.

Das mit den Updates wird sich noch zeigen.

Beitrag von „MacPeet“ vom 23. November 2021, 00:54

Ich bin noch nicht ganz schlau daraus geworden, worum es hier geht. OCLP-Patches auf einem Hackintosh anwenden, richtig?

Wenn ja, dann kann man auch den PostInstall-OCLP in der GUI selbst anschubsen, sofern man das richtige SMBIOS dort eingestellt hat, selbst wenn man nicht selbst mit OCLP bootet, sondern beispielsweise mit dem normalen OC für den Hacki oder gar Clover.

Hat griven bereits so gemacht, vor einiger Zeit, was in einem anderen Thread stand.

msart

Durchaus möglich, was Du da schreibst. Die Kepler-Treiber sind ja quasi nur ein Rollback von da, wo es noch nativ ging, also vor 12.1 DP1 (hier sind die Nvidia-Kext's geflogen).

Die Kext's sind aber unverändert, so dass die Signatur der Kext's (oder wie Ihr schreibt Siegel gebrochen) nicht verändert wurde. Somit sind die noch immer nativ Apple signiert und sollten auch mit aktiviertem SIP geladen werden.

Veränderte Kext's konnte man früher im Terminal sogar neu signieren mit "sudo codesign ... bla bla", was ich aber auch seit Catalina selbst nicht mehr brauchte.

Betreffs Hackintosh und diesen Patches kann ich sicher nicht mitreden, aber zumindest betreffs meinem MacPro3,1 kann ich mitreden, der ja auch inzwischen all diese Patches braucht.

Das zurückspielen der Nvidia-Kext's braucht der auch, da er eine Nvidia-Metal-Karte hat. Ferner braucht der auch den neuen rdrand-Patch wegen der CPU.

Ferner auch die Broadcom-Patches für BT, da die real ...CD zwar noch nativ WLAN bringt, aber BT ansonsten gebrochen ist.

Die Aussage, dass man mit all diesen Patches keine OTA-Direktupdates mehr fahren kann, ist so vielleicht nicht ganz richtig, zumindest lief bei mir jedes Direkt-Update ohne zutun durch, brauchte also keinen FullInstaller.

Evtl. ist dies aber auch auf'm Hacki anders, durchaus möglich.

Beitrag von „5T33Z0“ vom 23. November 2021, 10:01

MacPeet

Zunächst einmal: Meine Beschreibung, was hier gemacht wird ist ziemlich eindeutig und präzise: Booter- und Kernel Patches auf LEGACY PC HARDWARE verwenden, die die Virtualisierungsfunktion von Monterey nutzt, um macOS 12 eine unterstützte Board-ID

vorzugaukeln, während die Hardware aber das für sie angemessenes SMBIOS verwendet, um so MacOS Monterey installieren, starten und updaten zu können – mit einem offiziell nicht unterstützten SMBIOS.

1. Dein Argument, die Patches erst "im Post-Install anzustoßen" scheitert schon im Ansatz, da es sich WIE MEHRFACH erwähnt, hier um Booter- und Kernel-Patches handelt, die bereits beim Laden von OpenCore angewendet werden müssen! Ohne sie wären Boot, Installation und Update von macOS Monterey auf Legacy PC Hardware unmöglich. Abgesehen davon: da diese Booter und Kernel Patches aus der config.plist von OCLP stammen, handelt es sich dabeu eh um Patches, die beim Laden von OpenCore angewendet werden – auch bei nem Mac. Von daher kann man das auch nicht im Post-Install mit irgendner GUI machen. Bitte nicht Dinge zusammenwürfeln, die nichts miteiander zu tun haben!

2. Bezüglich Delta Updates: es geht nicht darum, ob die Signatur der nachträglich rein gepatchten Treiber in macOS Monterey korrekt ist, sondern darum dass das Siegel der Snapshot Partition dabei gebrochen wird. Und deswegen funktionieren Delta Updates danach nicht mehr. Ich habe einen PC und ein Laptop die mittlerweile beide nachträglich reingepatchte Treiber benötigen. Im ersten Fall Kepler und im zweiten IntelHD4000. Und in beiden Fällen sind danach keine Delta-Update mehr möglich. Vielleicht ist das auf vintage Macs anders, aber um die geht es hier nicht. Ob Delta Updates funktionieren ist eh sekundär für mich. Es geht darum, das der Board-ID spoof funktioniert.

Ganz ehrlich: bevor Du mich kritisiert, solltest Du zunächst verstehen, worum es in der Sache geht, aber das hast Du nicht. Du siehst "oh OCLP Patches" und denkst an alte Macs. Darum geht es aber hier ganz und gar nicht. Denn sonst wäre dieser Thread vollkommen überflüssig. Es geht immernoch um Hackintoshes. Es ist halt wieder typisch deutsch, dass einem statt "oh coole Idee" hier nur wieder "was soll das?" entgegenschlägt – bei vollkommener Unkenntnis der Sachlage. Anstatt erstmal anzuerkennen, was jemand hier anbietet. Frustrierend.

Beitrag von „MacPeet“ vom 23. November 2021, 10:49

Kritisiert habe ich Dich überhaupt nicht, frage mich, warum Du Dich immer gleich angegriffen fühlst.

Natürlich braucht es viele Patches bereits im Bootloader für die Legacy-Hardware.

Wie genau und wann spielst Du denn die Kepler- bzw. IntelHD4000-Treiber ins System ein?

Dies bezüglich meinte ich ja auch nur, dass man dafür auch den PostInstaller vom OCLP-Patcher nutzen kann, selbst wenn man OCLP nicht als Bootloader nutzt, was hier bereits erfolgreich gemacht wurde.

OC oder OCLP basiert letztlich auf dem gleichen Loader und nach Boot im System ist es egal, ob PC oder Mac, verhalten sich beide gleich.

Dieses wird ja erst im System selbst ausgeführt. Nach Updates ist man erst einmal im Vesa-Mode, da z.B. die Nvidia-kext's noch fehlen.

Der Postinstaller spielt diese dann wieder ein, erneuert den Kernelcache und erstellt den neuen Snapshot, ohne dass dieser gebrochen wird.

Es geht dabei auch nur darum, die fehlenden Kext's wieder sauber ins System zu bekommen. Unterschiede betreffs PC oder realMac gibt es bei dieser Ausführung nicht.

Selbstverständlich hat es nicht's mit den Patches zu tun, welche bereits der Bootloader braucht.

Beitrag von „5T33Z0“ vom 23. November 2021, 11:57

Deine Äußerungen beziehen sich nicht auf den Kern des Themas Board-ID Spoof mit Virtzalisierungsmöglichkeiten von macOS Montere, sondern auf Post-Install, was mit diesem Guide nichts zu tun hat!

Der board-id spoof ermöglicht erst, das System unter macOS 12 zu booten. Wie jemand danach seine Treiber installiert, muss sie/er selbst wissen. Sei es via Geforce Kepler Patcher, sei es via HD4000 Patcher oder manuell mit Hilfe Command Line Snapshot Mounter

Und meine Erfahrung ist: 1) boot nach reinpatchen der Treiber ist nur möglich mit dekativierter SIP möglich 2) delta Updates sind danach unmöglich.

Im OpenCore Legacy Patcher GUI gibt es keine separate Option, um nur Grafiktreiber zu installieren.