

OpenCore startet funktionierende EFI nicht mehr - ist das Board hin ?

Beitrag von „griven“ vom 24. Juni 2021, 14:37

Korrekt ohne wird ein Zufallswert erzeugt und genau das ist ja auch der Sinn der Sache. Der Adress Space des Kernels soll ja gerade bei jedem Boot um einen zufälligen Wert (Offset) verschoben werden. Der Parameter Slide=XX gibt hebt genau diesen Zufall aber aus indem er einen festen Offset vorgibt (Slide = 0 wäre kein Offset und damit gleichbedeutend mit KASLR Fehlanzeige). Wenn Du auf den Parameter verzichtest und OC machen lässt (provide custom slide Quirk ist eingeschaltet) ermittelt OC im Vorfeld welche Offsets in Frage kommen und erzeugt aus diesem Pool einen zufälligen Wert was die Chance auf einen erfolgreichen Boot erheblich erhöht.