

macOS 13 VENTURA beta

Beitrag von „griven“ vom 5. November 2022, 11:50

[Zitat von ozw00d](#)

Wenn ich dich richtig verstehe macht das auch nur beim oclp sinn.

Es macht immer dann sinn wenn man tief ins System eingreifen (muss) und ggf. Systemdateien austauschen oder dahingehend verändern muss das deren Integrität nicht mehr gegeben ist. Im normalen Betrieb macht man das in aller Regel nicht bzw. wenn doch dann tut man das am System vorbei (Kext Injektion via OC zum Beispiel). AMFI verrichtet seinen Job in dem Moment in dem ein File geladen wird zum Beispiel ein Framework oder eine Library wie gesagt im normalen Betrieb kein Problem denn selbst wenn hier Patches benötigt werden dann passiert das im Speicher das physische File auf der Platte bleibt davon unberührt und somit auch dessen Zertifikate etc. pp. gültig. Aber generell und in 99,9% aller Fälle kann man der Aussage "es macht nur beim oclp sinn" zustimmen denn warum sollte man ein relevantes Sicherheitsfeature aushebeln und so sein System ohne Not schwächen wollen?