

Erledigt

## Gerade auf Heise

Beitrag von „kuckkuck“ vom 12. Februar 2020, 17:00

[Zitat von ozw00d](#)

OC: verlinkt die Kext quasi während der Laufzeit als wenn der kext aus dem cache kommt (prelinked)

Ich weiß nicht was du mit "während der Laufzeit meinst", aber man kann es sich in etwa so vorstellen. Normalerweise packt macOS selber alle Kexts in einen Cache und lädt dann beim Start die Daten ohne große Verifikation (die passiert soweit ich weiß größtenteils davor) aus diesem Cache. OC bastelt den Cache auseinander (ohne involvierung von macOS), fügt die vom Benutzer hinterlegten Kexts ebenfalls in den Cache, schnürt das Paket wieder zu und übergibt das ganze macOS. macOS lädt daraufhin alle Kexts aus dem Cache, wie als wäre nichts gewesen und genau so, wie es sein soll.

Clovers Injection basiert hingegen auf einer alten macOS Kernel-Methode, mit der es damals möglich war Kexts zu laden, obwohl sie nicht im oben genannten Cache liegen. Diese Methode ist veraltet und unbenutzt, warum sie noch im Kernel vorhanden ist weiß ich persönlich nicht. Da es dazu aber offensichtlich keinen Grund gibt, kann die Methode auch jederzeit verschwinden und Clovers KextInjection ist hinüber...

Edit: DF war schneller, aber vielleicht hilft ja meine vereinfachte Darstellung dem ein oder anderen es zu verstehen...