Anleitung für Broadcom-WLAN-Patch unter macOS Sonoma

Beitrag von „mhaeuser“ vom 11. September 2023, 10:39

> Zitat von macinsane
>
> It is just funny that one of the major selling points of OC was, that we never will have to alter SIP. The irony.

No clue what this rubbish is about, but maybe another history lesson is in order. SIP was never a major concern during the development of OC, because it just works, even with Clover. It is a feature enabled by efiboot and XNU that does not require any level of support or such. It is important to note that, by default, Clover disables SIP for no particular reason, but you can configure it to enable it. It also is important to note that without Secure Boot and something like OC Vault, write access to the ESP is enough to disable SIP, which can be achieved from auto-booting a malicious EFI app from an arbitrary FAT32 volume. What *was* a major selling point of OC is the prelinking-based kext injection, which became mandatory as of 11+ and has thus been integrated into Clover as well.

Regarding unsigned kexts and injection: Unsigned kexts are a problem if and only if they are installed within macOS. All kexts are prelinked nowadays and this process invalidates the digital signature. As such, there is no signature verification of third-party kexts at runtime, but only at build-time, no matter the boot solution. Injected kexts are prelinked at runtime by OpenCore or Clover and they are not subject to signature verification under any circumstances (OC may manually verify them as part of OC Vault). Most kexts can be injected, but especially with downgrades things are not always as easy. If you downgrade kexts that other kexts depend on, this would require relinking all of their prelinked symbols, which is not supported as of now. This pretty much is the only known case where you have to reduce SIP, as done by OCLP for some machines.

Regarding frameworks and such: This is out of the scope for *any* bootloader. No, team Clover cannot save you, because frameworks are loaded way past the exit-time of both OpenCore and Clover. I'm frankly not firm with the exact issues of AMFI (but unlike the kext injection scenario, there *is* signature verification of dynamic libraries at runtime), but I know that the people working on it are. So while any mitigation of the SIP downgrade situation by either OC or Clover is categorically infeasible (and both have nothing to do with frameworks to begin with), I assume AMFIPass is as good as it gets with it right now.

If SIP is your only concern, no clue what keeps you from using Clover right now. But if your goal is to get rid of OC's implementation details or Acidanthera software in general, I am afraid you are all out of luck.