CFG Lock

Beitrag von „Brumbaer“ vom 8. September 2020, 00:47

CFGLock.efi ist kein Hack oder Patch. CFGLock.efi verwendet eine vom BIOS vorgesehene Methode um einen Wert zu ändern.

Der Vorteil ist, dass CFGLock.efi "sicher" ist und am BIOS nichts verändert, was ein CMOS Reset nicht reparieren kann.

Der Nachteil ist, dass wenn der Wert bzw. die Methode nicht vorhanden sind, funktioniert CFGLock.efi nicht.

CFGLock.efi sucht bestimmte Pfade ab. Es ist denkbar, dass eine entsprechende Option auf einem anderen Pfad liegt, aber ich weiß es nicht.

PP0 bezieht sich auf eine RAPL Domain. Das hat mit Powermanagment zu tun und nichts mit dem CFG Lock um das es uns geht.

cga

CFGLock.efi kann keine Bytemuster finden und patchen, dazu ist es nicht gedacht. Wäre es so würde ich es nicht der Allgemeinheit zur Verfügung stellen, weil der Benutzer leicht Probleme erschaffen kann, die sich nur durch ein Neuladen des BIOS beheben lassen. Und nicht jedes Mainboard hat eine Option, die das auch bei zerschossenem BIOS zulassen.