

CFG Lock

Beitrag von „cga“ vom 6. September 2020, 21:09

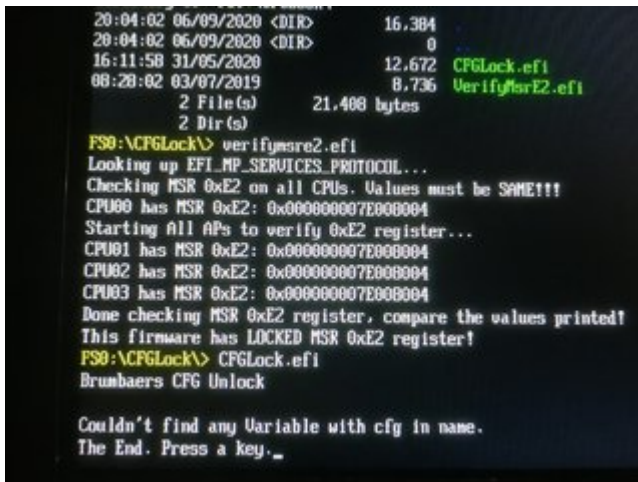
Hallo

Ich habe einen Intel NUC6 (NUC6i5SYK) mit BIOS 072 (<https://downloadcenter.intel.c...SKLi35-86A-?product=89190>).

Ich habe Ihr vielversprechendes Angebot ausprobiert und den folgenden Fehler erhalten:

Code

1. Couldn't find any Variable with cfg in name.
2. The End. Press a key.



```
20:04:02 06/09/2020 <DIR>          16,384
20:04:02 06/09/2020 <DIR>              0
16:11:58 31/05/2020          12,672  CFGLock.efi
08:28:02 03/07/2019           8,736  Verifyfsmre2.efi
      2 File(s)          21,408 bytes
      2 Dir(s)
FS0:\CFGLock> verifyfsmre2.efi
Looking up EFI_MP_SERVICES_PROTOCOL...
Checking MSR 0xE2 on all CPUs. Values must be SAME!!!
CPU00 has MSR 0xE2: 0x000000007E000004
Starting All APs to verify 0xE2 register...
CPU01 has MSR 0xE2: 0x000000007E000004
CPU02 has MSR 0xE2: 0x000000007E000004
CPU03 has MSR 0xE2: 0x000000007E000004
Done checking MSR 0xE2 register, compare the values printed!
This firmware has LOCKED MSR 0xE2 register!
FS0:\CFGLock> CFGLock.efi
Brumbaers CFG Unlock

Couldn't find any Variable with cfg in name.
The End. Press a key._
```

Funktioniert es nicht für Intel NUCs oder NUC6? Kann ich Ihnen beim Debuggen helfen? Seltsamerweise kann das Tool verifyfsmre2.efi erkennen, dass es gesperrt ist.

Vielen Dank im Voraus für Ihre Hilfe!

cga