CFG Lock

Beitrag von „Brumbaer“ vom 31. Mai 2020, 16:33

Bei manchen Boards gibt es keine Option um CFG Lock abzuschalten.

Die Bootloader haben Optionen um das zu umgehen, aber schön ist anders.

Es gibt im Netz eine Anleitung, wie man mir UEFI Tool, ifrextract und einem modifizierten Grub, CFG Lock löschen kann. Nicht nur dass schön anders ist, es funktioniert auch nur, wenn die Option in einem bestimmten VarStore gespeichert ist. VarStore ? egal.

CFGLock.efi ist eine EFI Tool, dass man in Opencore einbindet (in Tools auf der EFI Partition kopieren und in der config.plist unter Misc->Tools eintragen) oder über eine EFI Shell startet (habe ich nicht probiert, sollte aber gehen).

Das Opencore muss nicht in der Lage sein macos zu starten, es muss nur seinen Picker öffnen können.

Dort wählt man das Tool an und lässt es arbeiten.

Wenn CFG Lock als Option vorhanden ist - versteckt oder nicht - wird es angezeigt und man gefragt ob man den Wert ändern möchte.

Wenn man y oder Y (möglicherweise z bzw. Z) wählt wird CFG Lock umgeschaltet (von aus auf an bzw. von an auf aus - dass sagen wir jetzt 10 mal schnell hintereinander).

Danach neustarten.

Ich habe nur Mobos von ASRock und Gigabyte zum Testen hier, bei beiden geht es.

Falls es einer einsetzt, wüsste ich gerne ob es geklappt hat - sprich das MoBo eine CFG Lock Option hat.

CFGLock.efi.zip

Beitrag von „theCurseOfHackintosh“ vom 31. Mai 2020, 16:39

Klingt schon mal gut und danke für das tool!

Um den CFG-Lock (oder auch Msr0XE2 Lock) zu deaktivieren, kann man auch "UefiPatch" verwenden, dann muss man aber ein BIOS flashen.

Aber, was ich nicht verstehe:

Wird mit diesem Tool dann eine Einstellung im Uefi freigeschaltet, oder nur der Wert geändert?

Beitrag von „Brumbaer“ vom 31. Mai 2020, 16:53

Nur der Wert geändert.

Beitrag von „theCurseOfHackintosh“ vom 31. Mai 2020, 16:54

Ok. Dann ergibt es Sinn für mich

Beitrag von „Toskache“ vom 31. Mai 2020, 17:35

Funktionier hier bei meinem Gigabyte Z390 Designare einwandfrei!

Beitrag von „Doctor Plagiat“ vom 1. Juni 2020, 17:23

Brumbaer Funktioniert ausgezeichnet mit dem Dell-XPS15.

Beitrag von „badbrain“ vom 1. Juni 2020, 18:38

Funktioniert beim Z490 Vision D - danke.

EDIT: Ebenso beim Z390 Aorus Master

Beitrag von „Mork vom Ork“ vom 1. Juni 2020, 19:29

ASRock X299 OC Formula: works

Beitrag von „luxus13“ vom 1. Juni 2020, 20:59

Vielen Dank, einfach perfekt.

GA-Z170X-UltraGaming

Edit:

GA-Z170-HD3P. ... ebenfalls

```
Looking up EFI_MP_SERVICES_PROTOCOL...
Checking MSR 0xE2 on all CPUs. Values must be SAME!!!
CPU00 has MSR 0xE2: 0x000000001E000006
Starting All APs to verify 0xE2 register...
CPU01 has MSR 0xE2: 0x000000001E000006
CPU02 has MSR 0xE2: 0x000000001E000006
CPU03 has MSR 0xE2: 0x000000001E000006
Done checking MSR 0xE2 register, compare the values printed!
This firmware has UNLOCKED MSR 0xE2 register!
```

Beitrag von „tecnicasopr“ vom 4. Juni 2020, 19:05

Bedankt voor je tool. Het werkt met GA-Z170X-Gaming G1

Beitrag von „JimSalabim“ vom 4. Juni 2020, 22:53

Funktioniert perfekt. Z390 Designare. Hat direkt erkannt, dass ich den Lock eh schon (über GRUB) entfernt hatte, also den Wert 0 ausgegeben. Habe dann zum Testen auf 1 geändert, Lock also wieder aktiviert und konnte so wie erwartet macOS auch nicht mehr booten. Wieder den den Wert auf 0 setzen lassen, Neustart und zack gehts wieder. Danke für das Tool, das macht es wirklich entschieden einfacher!

Beitrag von „pstr“ vom 5. Juni 2020, 08:46

JimSalabim gerüchteweise sollen die nächsten Gigabyte BIOS Versionen den CFG Lock wieder als BIOS Option enthalten. Ich habe hier bereits eins für das z390 Aorus Pro .

Mit diesem Tool aber nicht mehr so wichtig , funktioniert gut 👍

Beitrag von „vit9696“ vom 6. Juni 2020, 11:45

Brumbaer great job! Mind contributing to OpenCorePkg and merging with VerifyMsrE2?

Beitrag von „karacho“ vom 6. Juni 2020, 12:29

vit9696 That would be nice.

Beitrag von „Brumbaer“ vom 6. Juni 2020, 16:42

> Zitat von vit9696
>
> Brumbaer great job! Mind contributing to OpenCorePkg and merging with VerifyMsrE2?

I don't mid.

How to go about it ?

Beitrag von „vit9696“ vom 6. Juni 2020, 17:10

I would say we will need to rename VerifyMsrE2 to something like MsrE2Ctl and make it accept arguments like -check (and do what VerifyMsrE2 currently does) and -unlock/-lock (and perform your tool logic). Without the arguments it can possibly have some interactive mode.

A good start will be a PR of this change to OpenCorePkg. Then we could review and bring the changes to the project codestyle and such. For the arguments you can use GetArguments function from Library/OcMiscLib.h.

Thanks a lot!

Beitrag von „barrrrt“ vom 7. Juni 2020, 12:41

Bei meinem X570 Board gibt es anscheinend nicht eine solche Variable die geunlockt werden kann. Beim Start kam eine ähnliche Nachricht wie "no cfg variable found"...

Beitrag von „mhaeuser“ vom 7. Juni 2020, 12:43

barrrrt AMD-PM funktioniert anders und wird von macOS so oder so in keiner Weise unterstützt

---

Beitrag von „Iluvatar0“ vom 13. Juni 2020, 02:24

Zunächst erstmal vielen Dank für das Tool. Ich habe es auf einem ASUS X99-Deluxe II ausprobiert. Leider wird wie es aussieht an gleich zwei Stellen der CFG Lock gefunden. Die Ausgabe des Tools dazu füge ich bei.

Beitrag von „Brumbaer“ vom 13. Juni 2020, 02:52

Es ist keine der beiden Optionen.

Ich schau mal ob ich eine Kopie des BIOS bekomme. Falls ja überprüfe ich ob die Option vorhanden ist und wenn ja warum sie nicht gefunden wird.

Ich habe das BIOS von der Asus Seite runtergeladen. Das BIOS hat keine versteckte CFG Lock Option. Das Tool kann dann nicht funktionieren. Tut mir leid.

Weißt du ob CFG Lock gesetzt ist ? Wenn nicht, kannst du es mit VerifyMsrE2 kontrollieren. VerifyMsrE2 testet direkt das Register. Dummerweise kann man das Register nicht überschreiben sobald CFG Lock einmal gesetzt ist.

Beitrag von „Brumbaer“ vom 14. Juni 2020, 01:41

Könnt ihr bitte in einem anderen Thread weitermachen.

Beitrag von „Iluvatar0“ vom 14. Juni 2020, 01:57

Sorry, waren jetzt doch nen paar Beiträge am eigentlichen Thema vorbei. Es hat aber geklappt, MSR Register ist jetzt unlocked. Schuld war ein defekter Stick. Jetzt kommt der schwierige Part mit opencore. Bislang habe ich eine clover Installation mit nullcpupowermanagement. Vielen Dank

---

Beitrag von „marc31mo“ vom 14. Juni 2020, 08:25

darf ich fragen wofür das CFG Lock gut ist ?

Beitrag von „Brumbaer“ vom 14. Juni 2020, 13:28

CFG Lock ist ein Bit Prozessor internen Register E2 mit dem Namen MSR_PKG_CST_CONFIG_CONTROL.

Wenn einmal gesetzt bleibt es gesetzt bis zum nächsten Reset des Prozessors.

Ist es gesetzt können die untersten 15 Bit des Registers nicht mehr verändert werden.

Sind diese Bits aber "falsch" gesetzt hängt sich MacOs auf. Ist CFG Lock gesetzt kann MacOS die Werte nicht setzen und es ...

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

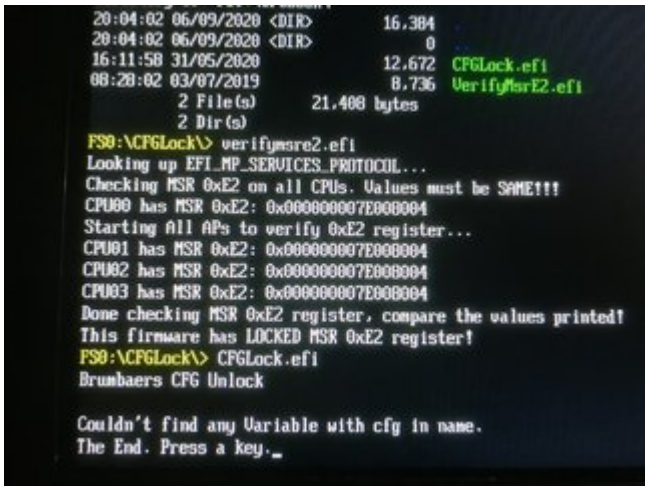
Hallo

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.



Funktioniert es nicht für Intel NUCs oder NUC6? Kann ich Ihnen beim Debuggen helfen? Seltsamerweise kann das Tool verifymsre2.efi erkennen, dass es gesperrt ist.

Vielen Dank im Voraus für Ihre Hilfe!

cga

Beitrag von „Brumbaer“ vom 6. September 2020, 22:14

cga

Das Programm sucht nach bestimmten Datenstrukturen, wie sie in aktuellen AMI BIOSen enthalten sind.

Die Fehlermeldung bedeutet, dass diese Struktur nicht gefunden wurde.

Da es sich um einen NUC handelt ist das wenig überraschend.

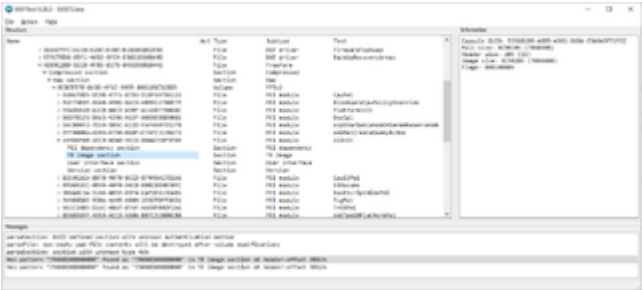
Ich habe keinen NUC um nachzuschauen ob man das Programm mit wenig Aufwand für den NUC anpassen kann. Tut mir leid.

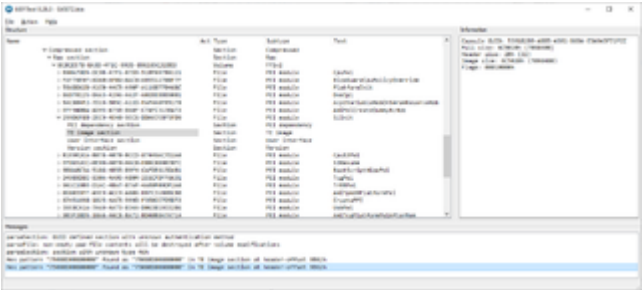
Beitrag von „cga“ vom 7. September 2020, 20:17

Vielen Dank für Ihr Feedback!

Nach diesem Verfahren (https://dortania.github.io/Ope...uide/extras/msr-lock.html) wurden in der Suche nach der Zeichenfolge "CFG Lock" keine Ergebnisse zurückgegeben.

Wenn Sie jedoch das Intel SY0072.BIO für diesen SkyLake NUC6 in UEFITool öffnen und nach SkyLake-spezifischen "75080D00800000" suchen (die gemäß UEFIPatch durch EB080D00800000 ersetzt werden müssen), finden Sie die folgenden 2 identischen Einträge:





Es scheint also, dass dieser MSR 0x2E-Registrer im "TE image section" in Intel BIO-Dateien enthalten ist. Dieser Offset in dieser speziellen BIO-Datei beträgt 9B62h. Kann das helfen?

Vielen Dank im Voraus für Ihr Feedback!

cga

Beitrag von „floris“ vom 7. September 2020, 21:06

ich hatte ja diesen Output von Bumbaers CFG Unlock gepostet.

Code

1. Brumbaers CFG Unlock
2. 1. 05 0F7A 0001 /MMCFG Base: IntelSetup
3. 2. 05 12AB 0001 /PP0 Current_Cfg_Ctl_ Ovrd/ VarStore Name: IntelSetup

4.
5. More than one CFG Variable found.
6. Do you want to select one of them ? _

Der erste Recherche-Versuch hat mich nicht schlauer gemacht, da ich nur zu MMCFG etwas fand - für ein Supermicro Board schaltet das irgend einen Memory-Bereich bei PCIe ...

Irgendwann ging ich dann den traditionellen weg, mit Clover Patches zu MSR 0x2E am Kernel (was jetzt soweit gut funktioniert) - aber:

bei den Kommentaren zu den Patches (von Pikeralpha) fand sich neben dem Begriff "CFG" auch der Begriff "PP0".

Meine versuche mit dem UEFITool waren nicht erfolgreich!!

Ich hatte vorher schon einmal in der UEFI update des Mainboards mit UEFITool nach dem Begriff "CFG" gesucht, aber bin nicht fündig geworden. (Trotz intensiver "Anstrengungen" ...)

Erst das Tool (über OC) von Brumbaer hat mir einen konkreten Hinweis gegeben, ob überhaupt "CFG lock" Variable(n) vorhanden sind.

Ich denke, das die Firmware/Datenstruktur irgendwie gepackt ist und sich nicht immer so einfach im "Binary" finden lassen.

Grüsse Florian

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.

Beitrag von „cga“ vom 8. September 2020, 10:25

Danke Brumbaer für deine Erklärungen. Ich verstehe jetzt besser, wie sich Ihr Werkzeug von anderen Methoden unterscheidet. Es sieht also so aus, als ob ich das MSR 0xE-Register nicht von meinem NUC entsperren kann. Ich muss dann die PM-Problemumgehungen in config.plist verwenden. Nochmals vielen Dank für Ihre Klarstellungen.

Beitrag von „NoBody_0“ vom 8. September 2020, 14:55

heute habe ich das Tool auf GB-Z170-hd3p und Latitude e7470 getestet und mit beiden hat es funktioniert...

Vielen Dank

Beitrag von „talkinghead“ vom 16. November 2020, 18:06

Brumbaer: Danke für das Tool. Läuft einwandfrei mit GB B360M-DH3.

Beitrag von „langweiler94“ vom 17. November 2020, 16:19

Vielen Dank für das Tool. Auf meinem Gigabyte Z370 HD3P läuft es ohne Probleme.

Beitrag von „TNa681“ vom 30. März 2021, 09:22

Nun läuft auch mein GA Z370 Gaming 7 mit OC und BigSur besten Dank an icecloud für den Tipp und die EFI und Brumbaer für das Tool!

Beitrag von „naujoks“ vom 19. Mai 2021, 09:56

Das hat super auf meinem Razer Blade Advanced 2021 Laptop funktioniert!

Kannst Du auch ein ähnliches Tool entwickeln, um DVMT Memory Size auf 64MB zu setzten? Das wäre genial! Die Razer Leute haben das BIOS fast völlig abgeschottet.

Beitrag von „Brumbaer“ vom 19. Mai 2021, 10:37

naujoks

Sorry, ich entwickle nur für den Eigenbedarf. Und wie so viele andere habe ich für die eigenen Projekte schon nicht genug Zeit 🙂

Beitrag von „pebbly“ vom 19. Mai 2021, 10:49

naujoks eigentlich ist es ziemlich einfach, wenn du mal diesem Guide gefolgt bist und statt cfg nach DVMT suchst: https://www.reddit.com/r/hacki...cking_alternative_method/

Beitrag von „naujoks“ vom 19. Mai 2021, 18:55

> Zitat von pebbly
>
> naujoks eigentlich ist es ziemlich einfach, wenn du mal diesem Guide gefolgt bist und statt cfg nach DVMT suchst: https://www.reddit.com/r/hacki...cking_alternative_method/

Das wäre eine tolle Sache, aber ich kann noch nicht einmal das BIOS extrahieren. UEFIExtract funktioniert überhaupt nicht. Und die Helden von Razer haben auch nicht das BIOS veröffentlicht, ich könnte also weder ein Backup anfertigen, noch das BIOS neu flashen, wenn etwas schiefgeht. Und nach DVMT suchen halt auch nicht.

Beitrag von „theCurseOfHackintosh“ vom 19. Mai 2021, 18:56

Wieso kannst du kein Backup anfertigen? Wozu verwendest du UEFIExtract?

Beitrag von „naujoks“ vom 19. Mai 2021, 19:16

Ich dachte UEFIExtract ist dazu da das BIOS zu dumpen?

Ich habe auch Universal IFR Extractor versucht, aber das funktioniert nicht, mit der Meldung "Protocol: unknown".

Versuche ich hier etwas Falsches?

Beitrag von „theCurseOfHackintosh“ vom 19. Mai 2021, 19:17

Nein... AfuWin oder FPT kann das. BIOS Programmer ist auch eine Möglichkeit, muss aber das Notebooks geöffnet werden.

Beitrag von „soniq“ vom 18. Dezember 2021, 18:26

es gibt ein neues Bios Update für das

Z370 AORUS Gaming 7

https://www.gigabyte.com/de/Mo...0/support#support-dl-bios

Jetzt bin ich auf der Suche nach einer "CFG lock" bzw. unlock gepachten Bios-Version?

P.S. Ja, ich weiß. In Open Core gibt es auch einen "CFG unlock" Schalter.

Beitrag von „Hecatomb“ vom 18. Dezember 2021, 20:10

soniq zb hier gibts welche... https://github.com/korzhyk/CLO…Gaming-7/tree/master/misc

---

Beitrag von „icecloud“ vom 18. Dezember 2021, 20:23

soniq

F15b funktioniert bei mir mit dem Z370 Aorus Gaming 7 gut. Entweder mit dem Tool von Brummbar hier oder mit der F15b Spezialvariante (CFG unlock Menüpunkt im Bios) eines Users im Tomatenforum. Google hilft hier beim finden.

habe mir auch überlegt auf das von Gigabyte dringend empfohlene F15 zu gehen. Leider ist das eine Capsuled Variante, d.h. zurück auf F15b für mich nicht möglich. Bei einem Hackintosh, der dann vielleicht nicht mehr rund läuft, für mich nicht zu empfehlen.

Beitrag von „schmalen“ vom 19. Dezember 2021, 08:10

soniq du könntest auch bei Gigabyte „esupport“ um eine modifizierte Bios Version anfragen. Habe eine bekommen wo „CFG-lock“ einstellbar war, allerdings für mein Aorus Master.

Beitrag von „icecloud“ vom 19. Dezember 2021, 08:55

schmalen

Guter Vorschlag mit dem Support von Gigabyte.

habe das gerade beantragt, nachdem ich im Bekanntenkreis jemanden gefunden habe der mir, trotz capsuled Bios, mein Bios auf 15b, zurückflashen könnte. Für den Fall das es als Hackintosh nicht rund läuft. Das hatte ich schon mit diversen Bios Varianten für das Aorus Gaming 7.

Bearbeitungszeit ist laut Gigabyte 3-7 Werktage. Vielleicht kommt ja was als Weihnachtsgeschenk.

Beitrag von „schmalen“ vom 19. Dezember 2021, 11:13

icecloud Aber.... bitte frage auch an, ob es mit dem veränderten Bios möglich ist, Updates oder Downgrades zu ermöglichen.

Ich hatte den Fall das ich kein Update installieren konnte Fehlermeldung "**"Oemid Mismatch" !"**, und mich wieder auf den eSupport verlassen musste, der auch schnell geholfen hatte.

Die Lieferung des Bios dauerte ca. 5 Tage

Gruss

schmalen

Beitrag von „icecloud“ vom 19. Dezember 2021, 11:27

schmalen

Danke für den Tipp. Mach ich.

Liebe Grüße

icecloud

Beitrag von „schmalen“ vom 21. Dezember 2021, 09:42

icecloud hast dein Bios schon erhalten?

Hatte auch ein Bios (aktuelles) angefragt (Zeitgleich) ist bei mir heute zum Download bereit.

Beitrag von „Hecatomb“ vom 21. Dezember 2021, 09:50

Krass wie einfach es doch sein kann mir eurer Anfrage

Beitrag von „icecloud“ vom 21. Dezember 2021, 14:13

schmalen

Habe eben nachgesehen.

Mein Bios ist auch da!

Kaum zu fassen wie kurz 5 Tage doch sind.

Bei all dem Weihnachtsstress komm ich aber erst nächste Woche dazu das einmal zu testen.

Beitrag von „icecloud“ vom 25. Dezember 2021, 10:36

Habe das erhaltene KundenBios 15 mit CFG_LOCK Ein/Aus Menüpunkt vom Gigabyte E-Support heute morgen installiert.

Alles schein Rundzulaufen.

Das Problem:

Major vulnerabilities updates, customers are strongly encouraged to update to this release at the earliest. Credits to "Assaf Carlsbad and Itai Liba from SentinelOne"

sollte damit erledigt sein.