

(Wie) bekomme ich CPU-Microcode-Sicherheitsupdates beim Hack?

Beitrag von „krokol“ vom 4. September 2020, 13:51

Hat jemand eine Idee, wie es um CPU-Microcode-Updates beim Hackintosh bestellt ist? Gerade hat Microsoft ein Windows 10 Update mit Microcode-Updates für Sicherheitsprobleme bei zahlreichen Intel-CPU's veröffentlicht, siehe [hier](#) und [hier](#). Normalerweise packt Apple solche Updates auch irgendwann in seine Installer (und teilweise landen sie natürlich auch in BIOS-Update, wenn es denn noch welche gibt).

Aber jetzt stellen sich mir diverse Fragen im Zusammenhang mit dem Hack:

- Bekomme ich diese Sicherheitsupdates auf einem Hackintosh via macOS überhaupt, wenn ich z.B. in OC Apple Firmware-Updates deaktiviere? (klar, ein CPU-Update ist kein Firmware-Update im strengen Sinn)
- Bekommt macOS überhaupt *alle* Microcode-Updates für die ganzen Prozessoren? Viele von uns nutzen ja CPU's die Apple nie verbaut hat.
- Wäre es sinnvoller, Windows (oder ggf Linux) mal zu installieren, um die Sicherheitsupdates zu bekommen und einmal einzuspielen? Oder sind die bei jedem Neustart wieder weg und müssen über das jeweilige Betriebssystem bei jedem Start neu geladen werden?

Früher hätte ich da keinen Kopf gemacht und höchstens auf ein BIOS-Update gewartet, aber ob die Hersteller da auch für alte Systeme wie meines noch was liefern ist eher fraglich. Da die Intel-CPU's sicherheitstechnisch mittlerweile aber eher Schweizer Käse gleichen, würde ich doch gerne erfahren, was "best practice" für einen Hack wäre.

Weiß jemand näheres?

LG Krokol

Beitrag von „Hecatomb“ vom 4. September 2020, 14:01

Kenne mich da leider auch nicht aus, aber installiert sich dieser Microcode iwo dann auf der

CPU, oder ist der im System verankert? Falls es auf der CPU gespeichert wird müsste es doch kein Problem sein auf einer separaten Platte halt mal kurz Windows mit deinem pc kurz zu installieren und zu updaten. Mehr kann ich dazu auch nicht beisteuern☹️

Beitrag von „Aluveitie“ vom 4. September 2020, 14:17

Microcode updates werden entweder vom BIOS oder vom OS geladen, nach einem Shutdown sind die wieder weg.

Beitrag von „floris“ vom 4. September 2020, 14:20

Microcode Updates können beim Booten (nach)geladen werden.

Mainboard Hersteller pflegen in ihre Firmware-Updates den Intel CPU Microcode ein.

Außerdem lässt sich CPU-Microcode bei manchen Betriebssystemen (Windows/Linux) beim Betriebssystemstart nachladen.

Vermute mal, dass Apple diese auch nachladen wird, da bei macOS Laufwerken oft eine Datei Firmware.scrap in der EFI vorhanden ist.

Beim Hackintosh wird man auf Updates vom Mainboard angewiesen sein, außer wenn die CPU ebenfalls von Apple verbaut wird, dann könnte die (technisch gesehen) nachgeladen werden ..

Beitrag von „ozw00d“ vom 4. September 2020, 14:31

Je nach dem welches OS du gerade nutzt entweder über Sicherheitsfixe oder Falls >Catalina

integriert, insoweit Apple diese halt integriert hat.

Beitrag von „5T33Z0“ vom 4. September 2020, 15:39

Sicherheitsupdates/patches unter macOS sind Bestandteil von Betriebssystemupdates.

Firmwareupdates von Apple beziehen sich auf System Management Controller (SMC). Da PCs so etwas nicht haben und der SMC bei Hackintoshes simuliert wird (mit FakeSmC und VirtualSMC.kext) kann man diese Updates getrost ignorieren und sich stattdessen das aktuellste [BIOS Update](#) für das verwendete Mainboard runterladen. Das enthält dann microcode updates für den jeweiligen Prozessortyp - sofern notwendig. Zuletzt glaube ich 2018 im Zuge das meltdown exploits. Das steht dann auch immer in der Beschreibung, was das Update enthält.

Dazu benötigt man nicht einmal ein Betriebssystem. Windows benötigt man ab und an, um Firmwares von SSDs oder sonst irgendwelchen Geräten upzudaten, falls es dafür keine Tools für macOS gibt.

Beitrag von „apfel-baum“ vom 4. September 2020, 16:15

hallo,

bei deiner hardware fehlt etwas- dein mainboard sowie dessen revision, so kann ich dir beispielsweise wenig bis garnicht sagen, ob man ein mcupdate soweit vorhanden in dein bios integrieren kann,wobei intel seine aufbereitungsform verändert hat- was eben die bereitstellung dieser angeht, aber wer weiß- laut artikeln sollen ja sogar ab sandy-bridge cpus etwas von update mitbekommen, unter win wäre das ein im artikel-von heise erwähnte KB4558130 -<https://support.microsoft.com/...0/intel-microcode-updates>

schön wäre es widerum auch wenn es intel "wie früher" auch als von *nux und co nachladbare datei bereitstellt, bei glück kommt die dann auch mit dem <https://github.com/platomav/MCExtractor> rein, so es das bios dann zulässt kann der aktualisierte mc dort eingepflegt werden. 😊 aktueller stand der db ist 158, und im changelog

steht nichts zu älteren cpus, also wie gesagt mit glück sind in der nächsten aktualisierung dann die "neuen" updates zu den älteren cpus mit drin.

lg

Beitrag von „cmoers“ vom 4. September 2020, 16:18

Bei Asus steht es in der Update-Beschreibung, falls vorhanden. (Im Fall meines Boards [vgl. 1502 / 1602](#))



Beitrag von „krokol“ vom 4. September 2020, 17:35



Merci an alle, die sich in diesem Thread beteiligt haben. Bestätigt weitgehend meine Überlegungen. Das aktuellste BIOS habe ich drauf, ist aber schon ein Jahr alt.

[apfel-baum](#) Das Motherboard des T20 ist mW ein Dell OEM Board, da kennt ich keine Modellbezeichnung bzw Revision.

Generell frage ich mich ja auch, wie kritisch diese CPU-Bugs wirklich sind bei der 0815-Nutzung als Hack. Aber ich will ja auch nicht, dass mir eine Webseite den ganzen Rechner übernehmen kann. 😡

Beitrag von „apfel-baum“ vom 4. September 2020, 19:41

ok, dell ist nicht so einfach glaube ich, da kannst auf dell selbst hoffen, das die am ball bleiben

Beitrag von „umax1980“ vom 5. September 2020, 08:24

Ein gewisses Risiko besteht aus meiner Sicht immer, gerade wenn die Auswahl der Internetseiten eben etwas mehr risikobehaftet ist. Damals die Meltdown Geschichte war schon sehr erschreckend, eben auch wegen des Umgangs mit dem Thema seitens Intel.

Ich halte BIOS möglichst aktuell, ob jetzt seitens des Betriebssystems etwas kommt sieht man ja in den Release-Infos des Updates.

Beitrag von „ozw00d“ vom 5. September 2020, 14:54

umax1980 mehr bleibt einem auch nicht möglich, das ist ja mit ein Grund warum RISC CPUs so im kommen sind, sind weniger anfällig für ne Grütze.