MSR Unlock/Cascade Lake Refresh Firmware Fix

Beitrag von „DSM2“ vom 23. März 2020, 02:24

Wie ihr sicherlich mitbekommen habt, gab es da einige Probleme in Bezug auf die Mainboards für die Cascade Lake Boards sowie,

neuen Bios Versionen falls diese ein ME/RC Update für die Cascade Lake CPUs beinhaltet haben, was zu ACPI Problemen führte und somit keine Installation oder ein Boot möglich war.

Davon abgesehen wurden die Werte für den Unlock verändert, was unter anderem dazu führte das 0xE2 MSR nicht unlocked werden konnte, selbst wenn euer Bios das Feature dazu besitzt, da die diese Werte in der Firmware nicht existierten.

Nach einigen Bug Reports sowie bitten das ganze doch im Bios zu fixen, hatte ich heute endgültig die Nase voll und habe mich an mhaeuser gewandt um das ganze zu fixen.

Die Lösung in Bezug auf den MSR befindet sich samt der benötigten Patches im Anhang unten und heißt UEFIPatch, welches eins der weiteren Projekte von keinem geringeren als vit9696 ist.

Dieses kleine aber sehr nützliche Tool begleitet mich bereits seit X99 Tagen und war in vielen Situationen ein sehr nützlicher Helfer, sobald es darum geht den MSR zu Unlocken.

Ich habe um euch den Prozess besser darstellen zu können ein kleines Video gemacht, worin ihr sehen könnt, wie ihr damit euer Bios patched.

https://youtu.be/aVGOf4cMQ_c

In meinem Fall war das Bios für ein Asus Motherboard mit Flashback Funktion, was es durchaus einfacher macht, dass Bios erneut zu flashen,

da hierbei keine Checksum überprüft wird, was das übliche vorgehen bei Mainboards ist, wenn das Bios mit dem üblichen Weg geflashed werden soll,

stimmt dieser Wert nicht mehr, so verweigert das Mainboard den Flashvorgang und man muss dies über Umwege realisieren.

Damit das Bios per Flashback auf das Board kommt muss das Bios File entsprechend nach Handbuch unbenannt werden was in diesem Fall X299E3.CAP bedeutet.

Anschließend auf einen USB 2.0 Stick packen und in den für den Flashback vorgesehenen Port einstecken und den Flashback Button für 3 Sekunden betätigen,

nach 3 Sekunden den Button loslassen und warten bis der Rechner den Flashvorgang abgeschlossen hat, dies kann durchaus etwas Zeit in Anspruch nehmen.

Während des Flashvorgangs blinkt die LED, sobald der Flashvorgang abgeschlossen ist, geht diese aus und ihr könnt euer System ganz normal booten und eure Einstellungen vornehmen.

Damit der ACPI Fehler ebenfalls behoben wird, einmal die SSDT aus dem Anhang, in eurer EFI hinterlegen und schon kann das Abenteuer beginnen.

Nachdem flashen ruhig mal verifizieren Das verifizieren habe ich mit OpenCore gemacht.

Beispiel anhand eines Cascade Lake X Boards (Asus Prime X299 A-II)

PS: nicht nur Workstations können damit unlocked werden, sollte euer BIOS dennoch gelocked bleiben, dann müssen die Patches noch für diese Platform in die Patches.txt hinterlegt werden.