[Sammelthread] MacOS BigSur 11.0 DEV-Beta Erfahrungen

Beitrag von „griven“ vom 5. September 2020, 22:46

badbrain *0x00000000 oder* AAAAAA== als Base64 kann man natürlich auch machen aber ehrlich gesagt braucht man dann auch gar keinen Wert in die config eintragen da der null Wert dem Standard unter macOS entspricht will meinen sie SIP ist vollkommen aktiviert

Der Key csr-active-config dient dazu die SIP ganz oder in Teilen zu deaktivieren hierbei setzt sich der Wert der hier eingetragen wird aus einer Bitmask zusammen wobei jedes Bit in der Maske für einen bestimmten Teil der SIP steht. Folgende Werte stehen zur Verfügung:

Setting	Wert in Hex	Bedeutung
CSR_ALLOW_UNTRUSTED_KEXTS	0x1	Erlaubt das Laden von nicht signierten Kernelextensions
CSR_ALLOW_UNRESTRICTED_FS	0x2	Ermöglicht den Zugriff auf eigentlich geschützte Systemverzeichnisse (/System/Library)
CSR_ALLOW_TASK_FOR_PID	0x4	Erlaubt Code Injects
CSR_ALLOW_KERNEL_DEBUGGER	0x8	Erlaubt das ausführen von Kernel Debuggern
CSR_ALLOW_APPLE_INTERNAL	0x10	Eine weitere Prüfinstanz, welche unsignierte Kexte blocken kann
CSR_ALLOW_UNRESTRICTED_DTRACE	0x20	Erlaubt das Ausführen von dtrace-basierenden Monitoring & Reporting Tools
CSR_ALLOW_UNRESTRICTED_NVRAM	0x40	Erlaubt das Bearbeiten oder Ändern des NVRAM's aus dem Userland
CSR_ALLOW_DEVICE_CONFIGURATION	0x80	Erlaubt die externe Konfiguration des Systems/Verhindert Updates über Apples SWSCAN wenn aktivert

CSR_ALLOW_ANY_RECOVERY_OS	0x100	Erlaubt "Downgrades des OS"
CSR_ALLOW_UNAPPROVED_KEXTS	0x200	Erlaubt das Laden von Extensions die zwar signiert aber nicht beglaubigt sind
CSR_ALLOW_EXECUTABLE_POLICY_OVERRIDE	0x400	Erlaubt das uneingeschränkte Ausführen von ausführbaren Dateien

Die Werte können beliebig miteinander kombiniert werden wobei jeweils der Hexadezimale Wert für jeden Teil der SIP den man deaktivieren möchte addiert werden muss. Angenommen wir möchten also zum Beispiel erlauben das nicht signierte (0x1,0x10) und nicht beglaubigte (0x200) Extensions geladen werden dürfen zudem möchten wir Debuggen können (0x8,0x20) und am NVRAM möchten wir auch rumspielen dürfen (0x40) es ergibt sich also 0x1+0x10+0x200+0x8+0x20+0x40 = 0x27100000 oder JxAAAA== im Base64 Format. Die SIP kennt also nicht nur die Zustände aktiviert oder deaktiviert sondern kann ganz im Gegenteil seht kleinteilig eingestellt werden nur leider macht das niemand wirklich bzw. nur die wenigsten machen sich Gedanken darüber was der unter csr-active-config eingestellt Wert wirklich bedeutet. Irgendwann hat sich in der Community die Denke etabliert das die SIP was ganz böses ist und daher grundsätzlich und immer deaktiviert gehört und fortan wird das halt so gefressen. Zuerst 0x67 später dann 0x7F und zu guter letzt aktuell halt 0x3E7 wurde zum Standart in jeder config und kaum jemand weiß für was oder warum der Wert da überhaupt gesetzt wird (ich gebe zu ich habe mir da auch nicht wirklich Gedanken zu gemacht bisher).

Ich möchte behaupten das die große Mehrzahl der User mit aktiver SIP (also kein Eintrag für csr-active-config) gut fährt und im normalen Betrieb auch kaum bis keine Einschränkungen bemerken wird dennoch gibt es immer mal wieder Situationen wo man einzelne Teile der SIP deaktivieren möchte/muss bei mir ist das zum Beispiel unter BigSur der Fall weil ich gerne meinen Adblocker (ADGUARD) auch unter BigSur verwenden können möchte was mit komplett aktivierter SIP nicht möglich ist. Die Funktionsweise von ADGUARD macht es nötig das eine Netzwerk Erweiterung installiert wird (Kext) was unter BigSur auf diese Art und Weise nicht mehr erlaubt ist (Stichwort DriverKit vs. KEXT) und von der SIP unterbunden wird so sie denn vollständig aktiv ist.