Verwendung von Homebrew

Beitrag von „HackMac1“ vom 10. August 2023, 09:09

Hallo zusammen,

auf Linux empfinde ich den Paketmanager APT eine wirklich Erleichterung. Applikationen können einfach installiert, zentral aktualisiert und deinstalliert werden. Für macOS existiert mittels Homebrew ebenfalls ein Paketmanager für den Mac. Nach der ersten Installation auf meinem M1 und mehreren App Installation bin ich Ansicht auch begeistert. Ich empfinde oft, dass die Update Möglichkeiten der Applikationen selber häufig nicht unbedingt auch Updates anzeigen.

Nun komme ich zum Aber. Nach mehreren Google Suchen und Reddit Beiträgen scheinen die Meinungen zu Homebrew und Co sehr auseinander zu gehen. Wie seht Ihr dies? Gibt es tatsächlich Risiken? Sogar Apple verwendet für die Installation des Gaming Port Toolkits Homebrew.

Beitrag von „apfel-baum“ vom 10. August 2023, 12:35

HackMac1 ,

ich finde homebrew sowie macports soweit ok, -unter win dann z.b. scoop oder auch chocolatery

lg

Beitrag von „talkinghead“ vom 10. August 2023, 18:51

Es kommt darauf an… ist meine Sicht.

Es hängt halt davon ab, ob/wo du die Pakete, die du brauchst, findest. Vor Ewigkeiten wollte ich ein Tool installieren und fandes in Homebrew nicht, dafür in Macports. Seitdem nutze ich macports. Allerdings ist es mir egal ob es brew oder port ist: ist das Paket mal installiert, dann kann man es i.d.R im Ökosystem auch aktualisieren/löschen.

Nachtrag:

https://apple.stackexchange.co…s-fink-and-homebrew#34972

Beitrag von „guckux“ vom 18. August 2023, 13:28

Guckux HackMac1

Risiken? Welche Risiken?

Das erste Risiko, welches Du eingehst, ist IT-Technik zu benutzen, die Krönung dessen ist dann iOT.

Differenzierter betrachtet, gibt es Meinungen, welche "kommerzielle" Herstellerprodukte befürworten (Bug-fixing, support). Hier an erster Stelle M$ (Millionen Fliegen können sich nicht irren), in den letzten Jahren häufen sich deren eklatante Sicherheitsprobleme, zu letzt bei dem Exchange Problem, ganz aktuell Azure365, wo eine chinesische Hackertruppe einen "Generalschlüssel" in die Finger bekam.

(Und wir wissen ja alle, wenn man ein kompromittiertes System betreibt, ist der einzig sichere Säuberungsweg ein kompletter Neu-Aufbau, aber sonst und darüber als solches hüllt M$ sein Schweigemäntelchen).

Ich bin aber auch recht überzeugt, daß es Apple mit MacOS oder - so es noch existent wäre - IBM mit OS/2, es nicht anders machen würden.

Die Software, angefangen beim Betriebsystem, über die Applikationen, werden immer komplexer und somit fehleranfälliger und sicherheitskritischer.

Ich arbeite seit >30 Jahren mit OpenSource. In solch einer langen Zeit gibt es immer wieder mal Produkte, welche auch nach langjähriger Pflege, eingestampft werden. Ist bei den kommerziellen aber auch nicht anders.

Sicherheitslecks gibt es auch hier immer wieder - und über Macports und Homebrew mag es möglich sein, sich auch mal codeveränderte Software auf den Rechner holen zu können. Die 30 Jahre haben aber auch gezeigt, daß die OpenSource Entwickler eine ganz andere Ethik haben, sie veröffentlichen idR ohne Kompromisse schnellstmöglichst entsprechende Kenntnisse über Lecks wie auch ein wesentlich schnelleres Fixing der Lecks. Ich habe hier den Eindruck, daß dergleichen Probleme, sei es security, wie auch Bugs, an ihrer "Ehre" kratzt.

Schönes Beispiel ist hier auch unser Sascha_77 , meist dauert es nur wenige Stunden (gefühlt Minuten), bis die Probleme gefixt sind - abgesehen von einem Support, von welchem sich die "Großen" eine Scheibe abschneiden könnten. DAS ist in meinen Augen "the way of OpenSource" - anders kenne ich es nicht.

So, jetzt nochmal meine Frage vom Anfang:

Welche Risiken meinst Du?

Beitrag von „apfel-baum“ vom 18. August 2023, 15:23

hallo guckux ,

streng genommen fängt das sicherheitsproblem sogar noch sehr viel weiter vorne bzw. tiefer?, an- bei den verwendeten cpus, iot soc auch gerne wie schon erwähnt. umso mehr code da ist, desto mehr schwachstellen können sich da mitunter einschleichen, code wird ja auch ausgelagert, bzw. gemeinsam beackert z.b. bei spielen. wenn da also ein kettenglied nen fehler macht.. ist mitunter der gesamte rest kaputt, bzw. ein einfallstor entstanden. bugs zu melden kann auch für den, der diesen gefunden hat schnell zu problemen führen, daher hat heise z.b. auch einen anonymen briefkasten erstellt. firmen mögen es nicht wenn sie darauf hingewiesen werden, das etwas nicht so läuft wiees soll, und sicherheitsprobleme in der "etablierten" soft- oder hardware sind. "offizielle" meldungen können sich nur die leisten, welche einen gesicherten hintergrund haben. der normaluser wird da schonmal mit interessanten schreiben bedacht.

im gegensatz zur closed source, bietet die opensource ja die möglichkeit eben den quellcode anzugucken, wenn man den lesen kann

wenn nun aber ein server mit kompromitierten software-paketen ausgestattet ist , ists eben auch doof, ggf. bekommt das der geneigte mündige nutzer dann schneller mit. -da gilt es eben auch, nicht blindlinks alle im internet stehenden befehle einzutippen, wenn man nicht weiß, was die machen.

lg

Beitrag von „pebbly“ vom 20. August 2023, 10:11

Code

1. brew upgrade --greedy -n
2. brew upgrade --greedy
3. brew cleanup

Sind super nützlich, um auf schnellem Wege seine Apps zu aktualisieren. (Die Über den AppStore natürlich dort).

Ein weiterer App-Tipp: https://max.codes/latest/

Andererseits verstehe ich die Frage auch nicht. Homebrew ist einfach klasse?