1400 - Death By 1000 Installers; on macOS, it's all broken!

Friday at 14:00 in Track 2
45 minutes | Demo, Exploit

Patrick Wardle*Chief Security Researcher, Synack*

Ever get an uneasy feeling when an installer asks for your password? Well, your gut was right! The majority of macOS installers & updaters are vulnerable to a wide range of priv-esc attacks.

It began with the discovery that Apple's OS updater could be abused to bypass SIP (CVE-2017-6974). Next, turns out Apple's core installer app may be subverted to load unsigned dylibs which may elevate privileges to root.

And what about 3rd-party installers? I looked at what's installed on my Mac, and ahhh, so many bugs!

Firewall, Little Snitch: EoP via race condition of insecure plist
Anti-Virus, Sophos: EoP via hijack of binary component
Browser, Google Chrome: EoP via script hijack
Virtualization, VMWare Fusion: EoP via race condition of insecure script
IoT, DropCam: EoP via hijack of binary component
and more!

...and 3rd-party auto-update frameworks like Sparkle -yup vulnerable too!

Though root is great, we can't bypass SIP nor load unsigned kexts. However with root, I discovered one could now trigger a ring-0 heap-overflow that provides complete system control.

Though the talk will discuss a variety of discovery mechanisms, 0days, and macOS exploitation techniques, it won't be all doom & gloom. We'll end by discussing ways to perform authorized installs/upgrades that don't undermine system security."
Patrick Wardle
Patrick Wardle is the Chief Security Researcher at Synack, and founder of Objective-See. Having worked at NASA and the NSA, and as well as presented at many security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Currently, Patrick's focus is on automated vulnerability discovery, and the emerging threats of OS X and mobile malware. In

his personal time, Patrick collects OS X malware and writes free OS X security tools.

@patrickwardle, objective-see.com

#defcon25/by_track/track2/friday #defcon25/By_Day/_Friday