What's New?

Todd McDaniel, Mac Group, Client Platform Services, Marriott Library

October, 2018

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

50 YEARS · ALL U NEED

https://www.gatesnotes.com/About-Bill-Gates/Remembering-Paul-Allen

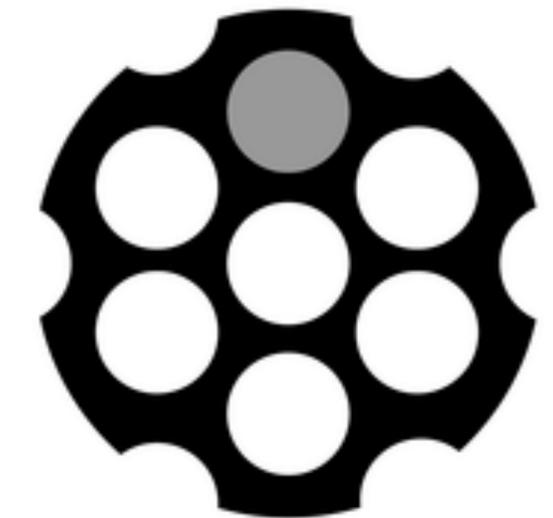https://www.wired.com/story/paul-allen-thought-like-hacker-never-stopped-dreaming/

iOS/iPhone security

iOS Security
iOS 12

September 2018

* https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

* https://risky.biz/RB514_feature/
Chris Wade, Corellium, an iOS emulator

RISKY.BIZ
It's a jungle out there

Authenticated Pointers and more...

✤ Multiple changes designed to avoid GrayKey/Celebrite types of unlocking

✤ Authenticated Pointers utilize extra bits to provide hashing, making buffer overflow/memory corruption exploitation much more difficult.

✤ Hardened DFU mode, Secure Enclave, Kernel

✤ Many of the previous methods will not work on new iPhones

Speaking of iPhones…

✤ Suspect forced to unlock phone using Face ID
https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face

✤ LEO's advised not to *look* at phones to avoid deactivating Face ID
https://motherboard.vice.com/en_us/article/5984jq/cops-dont-look-iphonex-face-id-unlock-elcomsoft

What is a supply chain attack?

✤ *A cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply network.*
https://en.wikipedia.org/wiki/Supply_chain_attack

✤ Examples:

   ✤ *Reflections on Trusting Trust*, Ken Thompson, 1984, modified `cc` backdoor

   ✤ NSA Tailored Access Operations (TAO) beacon installation, Snowden, ~2010

   ✤ Target breach, 2013

Bloomberg claims SuperMicro supply chain hacked

* https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
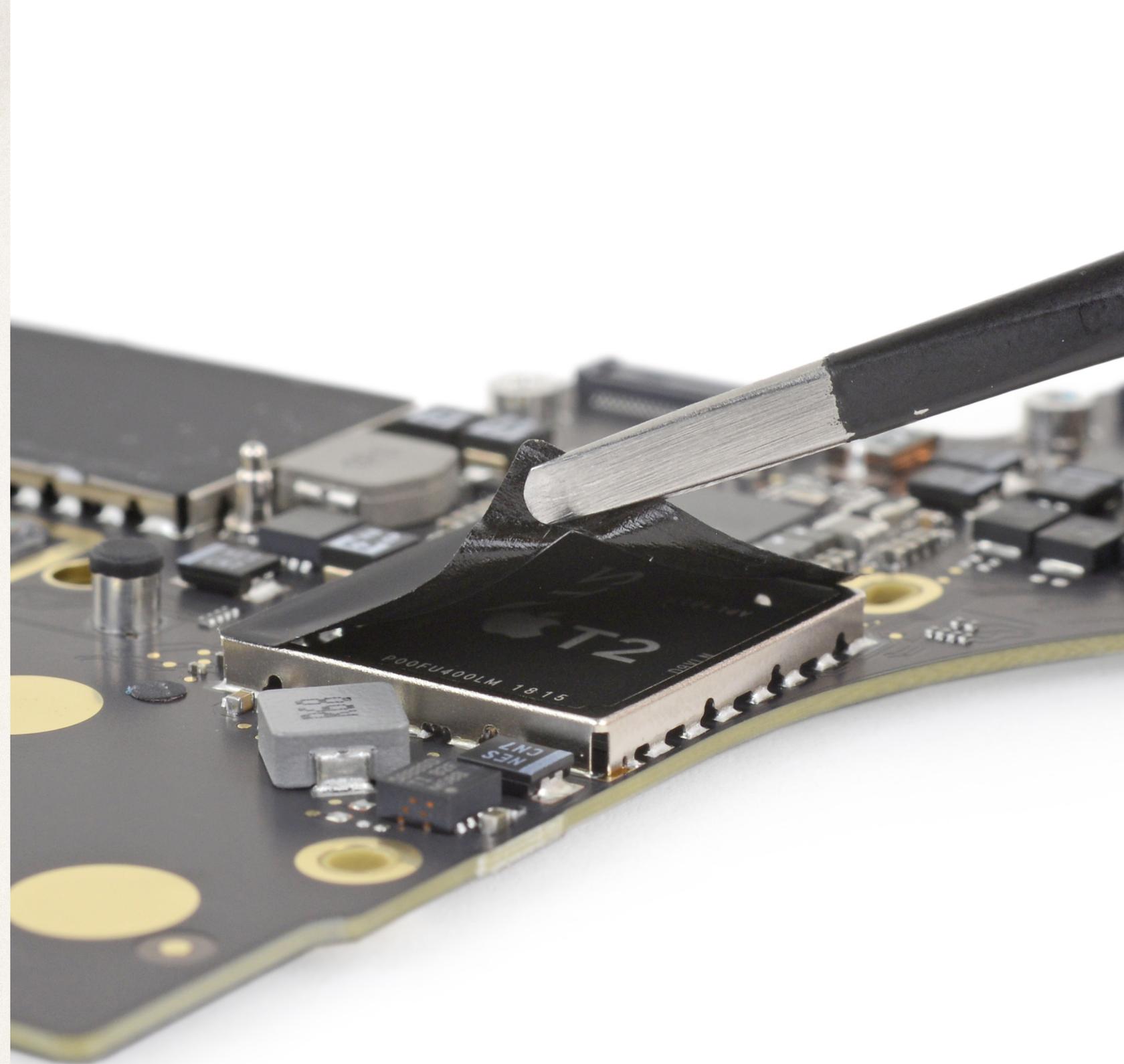
Apple & **many** others deny it's an issue…

- Those claimed to be affected deny the compromise took place
- Authors, publisher have written previous suspect IT stories
- 17 anonymous sources…
- No boards featuring suspect chip have yet been discovered
- History of problematic firmware…
  https://arstechnica.com/information-technology/2018/10/supermicro-boards-were-so-bug-ridden-why-would-hackers-ever-need-implants
- Risky Business Episodes: Interview with named source and #517

T2-equipped Macs require Apple Authorized repair, someday?

- 2018 MBP (Display, logic board, top case, Touch ID)
- iMac Pro (Logic board, flash storage)
- Apple Service Toolkit 2 required to "bless" replacement parts
- https://motherboard.vice.com/en_us/article/yw9qk7/macbook-pro-software-locks-prevent-independent-repair
- But testing shows locks not active?
  https://ifixit.org/blog/11673/t2-mac-repairs-test/
- What happens when they reach vintage status? Right to repair?

Facebook breach, again…

✤ Access tokens, searches, location data, profile info accessed

✤ Estimated at 50M, revised to 30M

✤ https://www.facebook.com/help/securitynotice?ref=sec
  Why make me scroll to the bottom of the page to find out?!?

✤ https://arstechnica.com/information-technology/2018/09/50-million-facebook-accounts-breached-by-an-access-token-harvesting-attack/

✤ https://arstechnica.com/information-technology/2018/10/facebook-hackers-stole-locations-and-other-private-data-for-millions-of-users/

Google+ to shutdown

✤ Launched in 2011, meant to compete with Facebook

✤ Ending service August, 2019
https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194

✤ Claiming low user adoption rates…

✤ And hole in the API, potentially exposing 500,000 accounts.

Microsoft Office 2019

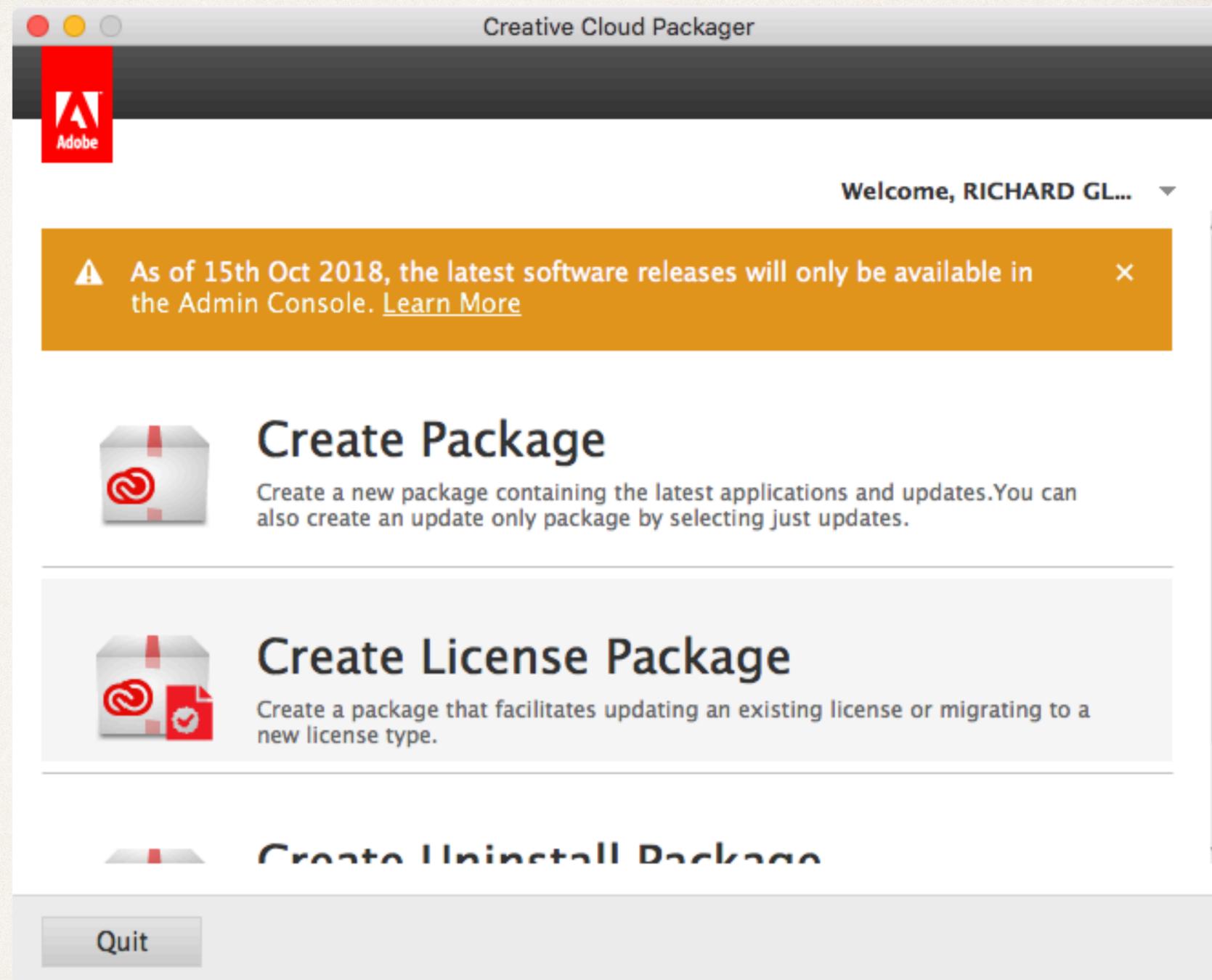* 10.12 is supported, going forward only current and previous two releases will be supported.
https://support.office.com/en-us/article/microsoft-changes-os-requirements-for-office-2019-for-mac-and-office-365-for-mac-16b8414f-08ec-4b24-8c91-10a918f649f8

Adobe CC 2019

✤ Elimination of serialized licensing…

   ✤ https://macmule.com/2018/10/15/adobe-creative-cloud-2019-the-death-of-creative-cloud-packager-device-licensing/

   ✤ https://gist.githubusercontent.com/macmule/9cc9d6cf0d311b846ee1a2cb3e45a04d/raw/018dde691a8a86b5113cf2607f1d363099d31300/gistfile1.txt

✤ Full Photoshop CC for iPad

Where are we now?

✤ Creative Cloud Packager is EOL. No more updates as of 10/15/18.

✤ Use the Adobe Admin Console to generate CC 2019 packages. Unless you have the old version of the portal, migration expected to complete by January, 2019

✤ Lab solution due Summer, 2019. Similar to device-based licensing, still requiring login.

Bill Lutz, OSL (7/30/18): Our previous Adobe Creative Cloud serial numbers, ending with -5522 and -2850, will expire and stop working on 11/30/2018. Our current active Adobe Creative Cloud serial number, which ends with -3169, will also expire on that date, ***but will continue to work when used in multi-lab and classroom environments that use concurrent user installations.*** However, after 11/30/2018, the active serial number will not provide access to the most recent versions based on the updated licensing technology.
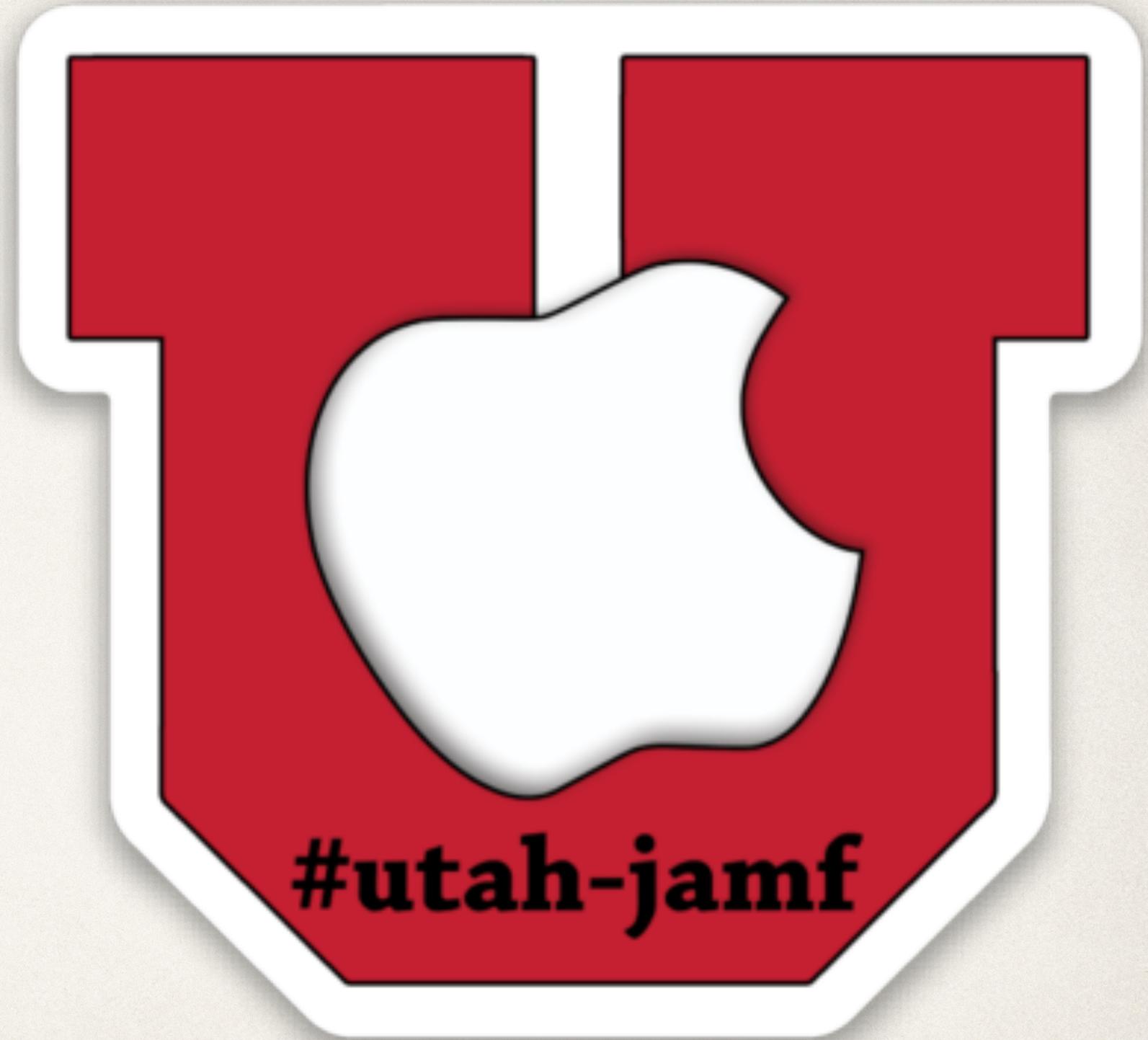
You can continue using the active serial number in multi-user lab and classroom environments, however, you must verify that you are using the active serial number that ends with -3169. Adobe will provide OSL with a transition solution in early 2019 for multi-user labs and classroom environments.

Richard Glaser (8/2/18): So, to be clear we will be able to get Adobe CC 2018 using a serial number, but NOT Adobe CC 2019 or until you have released a lab solution?

B. McNamara, Adobe (8/2/18): You are correct, your serialized lab deployments will not be eligible to update when we announce new version releases. Not until we have a lab solution in place in 2019.

JNUC 2018

- See you at the Pre-JUNC Meetup at Brits!
- Find us and ask for a sticker!

Questions, Comments?