

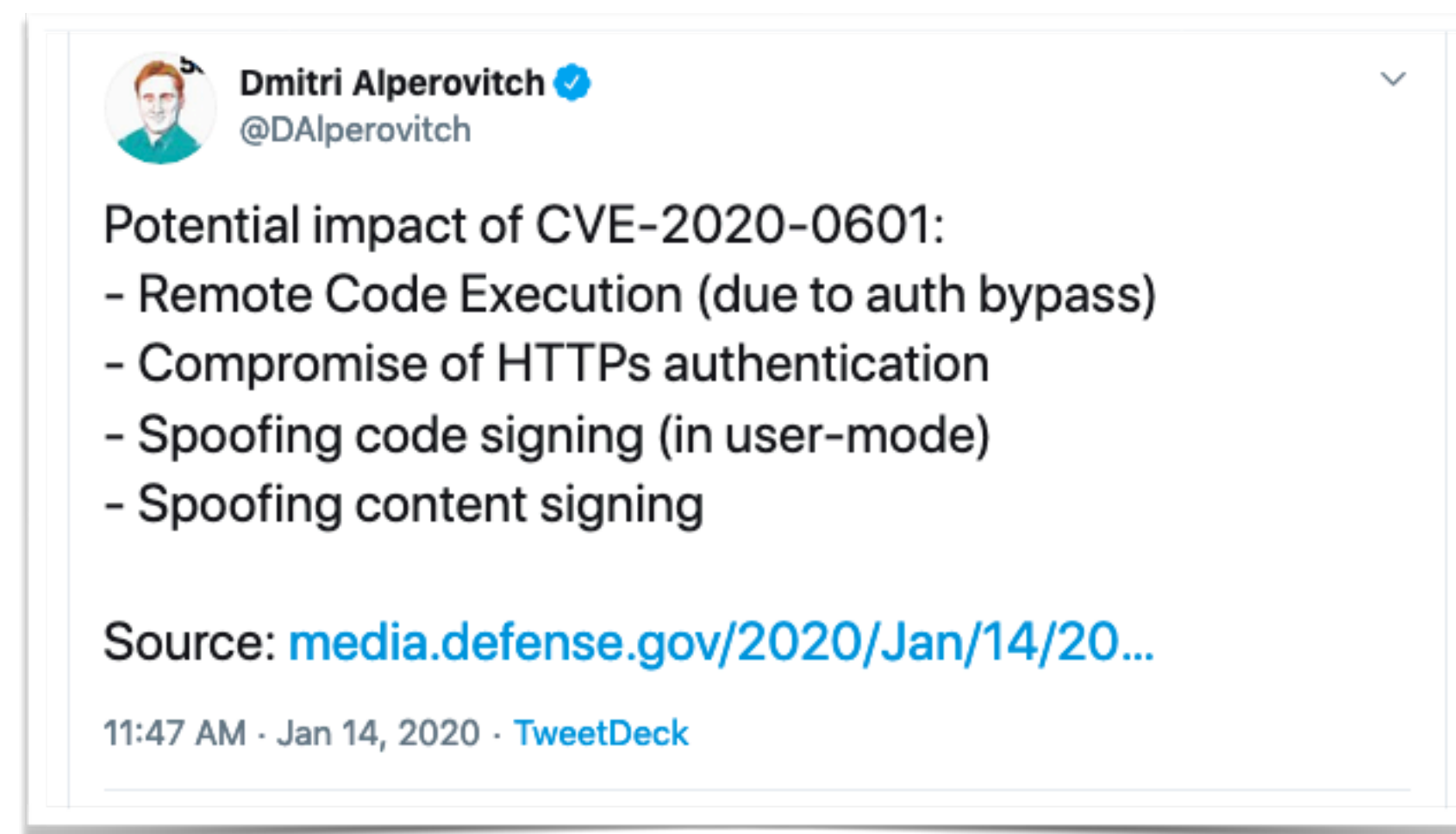
WHAT'S NEW?

Todd McDaniel

Mac Group, Client Platform Services, Marriott Library

SEVERE MICROSOFT CERT VALIDATION VULNERABILITY (CVE-2020-0601)

- <https://krebsonsecurity.com/2020/01/cryptic-rumblings-ahead-of-first-2020-patch-tuesday/>
- <https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2056772/a-very-important-patch-tuesday/>
- <https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF>



Customize your Mac Pro.

2.5GHz 28-core Intel Xeon W processor, Turbo Boost up to 4.4GHz

1.5TB (12x128GB) of DDR4 ECC memory

Two Radeon Pro Vega II Duo with 2x32GB of HBM2 memory each

4TB SSD storage

Stainless steel frame with wheels

Magic Mouse 2 + Magic Trackpad 2

Magic Keyboard with Numeric Keypad - US English

Processor

Which processor is right for you?

3.5GHz 8-core Intel Xeon W
processor, Turbo Boost up to
4.0GHz

- \$6,300.00

3.3GHz 12-core Intel Xeon W
processor, Turbo Boost up to
4.4GHz

- \$5,400.00

\$45,888.00

Continue



Get 6% Daily Cash back when you pay with Apple Card until
December 31, or get special financing >

IT COSTS HOW MUCH?!?!?

- \$22,500 worth of RAM
- ~\$10,000 worth of GPU
- Minus the \$1800 Afterburner card
- 8TB storage option coming soon!
- Rack mount option ordering now.
Starting at \$6,499
- EDU pricing, or lack there of

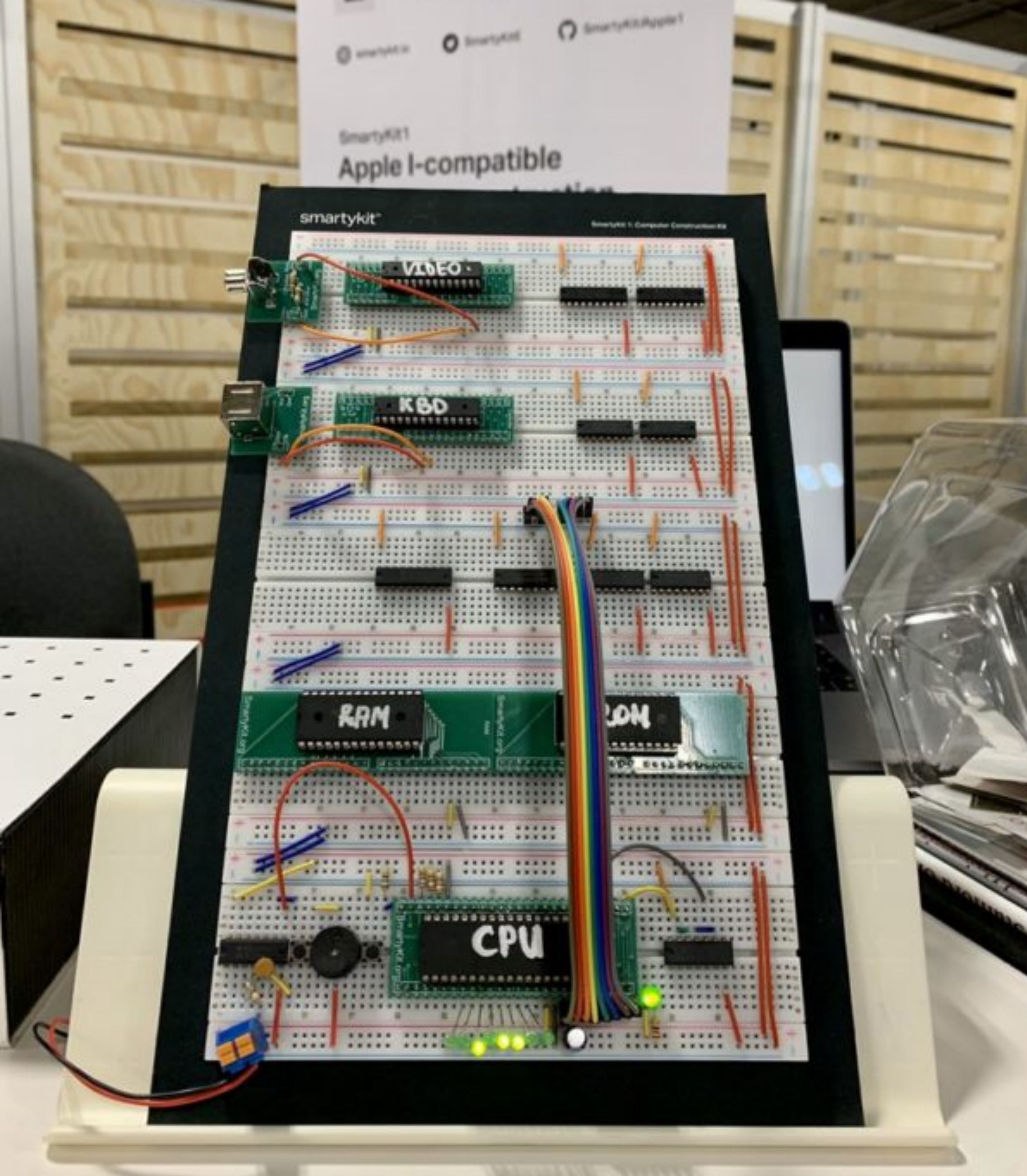
**BUT YOU FORGOT THE \$5,599
DISPLAY WITH THE \$899 STAND!**

PRO-MODE RUMOR

- <https://9to5mac.com/2020/01/13/macOS-beta-hints-at-future-pro-mode-to-boost-performance-on-portable-macs/>
- What about the reverse?
<https://marco.org/2020/01/13/macOS-low-power-mode-redux>

INDEPTH REPORT ON IOS 12.4 “SOCKPUPPET” ZERO CLICK EXPLOIT

- Address Space Layout Randomization (ASLR) weakness
- Use after free
<https://cwe.mitre.org/data/definitions/416.html>
- https://media.ccc.de/v/36c3-10497-messenger_hacking_remotely_compromising_an_iphone_through_imessage
- <https://googleprojectzero.blogspot.com/2019/12/sockpuppet-walkthrough-of-kernel.html>
- <https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-1.html>
- <https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-2.html>
- <https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-3.html>



DIY APPLE I

- <https://smartykit.io/>
- <http://osxdaily.com/2020/01/12/build-your-own-apple-i-replica-with-smartykit>
-

HACK DISCOVERED ONLY WHEN SERVER RUNS OUT OF DISK SPACE

- Infotrax, Orem, UT
- <https://www.zdnet.com/article/company-discovered-it-was-hacked-after-a-server-ran-out-of-free-space/>
- <https://arstechnica.com/information-technology/2019/11/breach-affecting-1-million-was-caught-only-after-hacker-maxed-out-targets-storage/>

WHY INFOTRAX?

InfoTrax® Systems, a trusted global name in **MLM software**, is an industry leading provider of backend operations systems and **online distributor tools** for the **Direct Sales** industry. From powerful software that integrates all mission critical operations to a suite of easy to use online independent distributor marketing, communication, and reporting tools, you get solutions that can support organizations from pre-launch start-ups to international **MLM Corporations** supporting millions of users.

FIREFOX TYPE CONFUSION 0-DAY (CVE-2019-17026)

- Version 72.0.1 contains the patch
- <https://arstechnica.com/information-technology/2020/01/firefox-gets-patch-for-critical-zero-day-thats-being-actively-exploited/>
- Type Confusion
<https://cwe.mitre.org/data/definitions/843.html>

NEW SHA1 COLLISION

- <https://sha-mbles.github.io/>
- <https://arstechnica.com/information-technology/2020/01/pgp-keys-software-security-and-much-more-threatened-by-new-sha1-exploit/>
- SHA1 still in use by git and for legacy support in other services

EUROPE HAS RUN OUT OF IPV4 ADDRESSES

- <https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses>
- <https://arstechnica.com/gadgets/2019/11/europe-is-fresh-out-of-ipv4-addresses/>

RSA-240 (795 BITS) FACTORED

- <https://arstechnica.com/information-technology/2019/12/new-crypto-cracking-record-reached-with-less-help-than-usual-from-moores-law/>
- <https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2019-December/001139.html>
- https://en.wikipedia.org/wiki/RSA_Factoring_Challenge
- https://en.wikipedia.org/wiki/RSA_numbers
- 900 core-years

RSA-240 =

1246203667817187840658350446081065904348203746516788057548187
8888328966680118821085503603957027250874750986476843845862105
4865537970253930571891217684318286362846948405301614416430468
066875699415246993185704183030512549594371372159029236099

or

**=509435952285839914555051023580843714132648382024111473186660
296521821206469746700620316443478873837606252372049619334517**

**2446242088383181505678131390240028966538020925789314014520412
21336558477095178155258218897735030590669041302045908071447**

MYSTERY DRONES!

- <https://www.nytimes.com/2020/01/01/us/drones-FAA-colorado-nebraska.html>
- <https://mailchi.mp/fde339578a4f/colorado-dhsem-releases-2019-colorado-state-emergency-operations-plan-1374537>
- <https://www.denverpost.com/2020/01/13/drones-colorado-public-safety-search-empty/>
- https://www.vice.com/en_us/article/pkeb9k/mass-panic-its-not-clear-that-colorados-mystery-drones-even-exist
- <https://www.nightdrones.net/>
“If enough of us are watching, we can figure this out.”



*Neil Peart
1952 - 2020*

COMMENTS, QUESTIONS?

