What's New February 2018

Todd McDaniel
Mac Group, Marriott Library, ITS

ALL U NEED

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

Spectre/Meltdown review

- Speculative execution - guess behavior in advance
- Meltdown mitigation - bug in speculative memory fetching, privileged memory
  OS/hypervisor patching, future CPU fixes
- Spectre mitigation - getting other programs to access the memory you want, branch prediction
  1 - *OS/Compiler patches*
  2 - *Javascript JIT/Browser updates*

Spectre/Meltdown updates

- Intel microcode updates released and retracted
- Microsoft complier patches, partially effective https://blogs.msdn.microsoft.com/vcblog/2018/01/15/spectre-mitigations-in-msvc/
- New variants: *MeltdownPrime and SpectrePrime: Automatically-Synthesized Attacks Exploiting Invalidation-Based Coherence Protocols* https://arxiv.org/pdf/1802.03802.pdf

Slow death of MacOS Server

- https://support.apple.com/en-us/HT208312
  List of deprecated services and alternatives
  “Removed in a future release”

Calendar	Contacts	DHCP
DNS	Mail	Messages
NetInstall	VPN	Websites
	Wiki	

LEAKED LIST OF MAJOR 2018 SECURITY VULNERABILITIES

CVE-2018-????? APPLE PRODUCTS CRASH WHEN DISPLAYING CERTAIN TELUGU OR BENGALI LETTER COMBINATIONS.

CVE-2018-????? AN ATTACKER CAN USE A TIMING ATTACK TO EXTPLOIT A RACE CONDITION IN GARBAGE COLLECTION TO EXTRACT A LIMITED NUMBER OF BITS FROM THE WIKIPEDIA ARTICLE ON CLAUDE SHANNON.

CVE-2018-????? AT THE CAFE ON THIRD STREET, THE POST-IT NOTE WITH THE WIFI PASSWORD IS VISIBLE FROM THE SIDEWALK.

CVE-2018-????? A REMOTE ATTACKER CAN INJECT ARBITRARY TEXT INTO PUBLIC-FACING PAGES VIA THE COMMENTS BOX.

CVE-2018-????? MYSQL SERVER 5.5.45 SECRETLY RUNS TWO PARALLEL DATABASES FOR PEOPLE WHO SAY "S-Q-L" AND "SEQUEL."

CVE-2018-????? A FLAW IN SOME x86 CPUs COULD ALLOW A ROOT USER TO DE-ESCALATE TO NORMAL ACCOUNT PRIVILEGES.

CVE-2018-????? APPLE PRODUCTS CATCH FIRE WHEN DISPLAYING EMOJI WITH DIACRITICS.

CVE-2018-????? AN OVERSIGHT IN THE RULES ALLOWS A DOG TO JOIN A BASKETBALL TEAM.

CVE-2018-????? HASKELL ISN'T SIDE-EFFECT-FREE AFTER ALL; THE EFFECTS ARE ALL JUST CONCENTRATED IN THIS ONE. COMPUTER IN MISSOURI THAT NO ONE'S CHECKED ON IN A WHILE.

CVE-2018-????? NOBODY REALLY KNOWS HOW HYPERVISORS WORK.

CVE-2018-????? CRITICAL: UNDER LINUX 3.14.8 ON SYSTEM/390 IN A UTC+14 TIME ZONE, A LOCAL USER COULD POTENTIALLY USE A BUFFER OVERFLOW TO CHANGE ANOTHER USER'S DEFAULT SYSTEM CLOCK FROM 12-HOUR TO 24-HOUR.

CVE-2018-????? x86 HAS WAY TOO MANY INSTRUCTIONS.

CVE-2018-????? NUMPY 1.8.0 CAN FACTOR PRIMES IN O(LOG N) TIME AND MUST BE QUIETLY DEPRECATED BEFORE ANYONE NOTICES.

CVE-2018-????? APPLE PRODUCTS GRANT REMOTE ACCESS IF YOU SEND THEM WORDS THAT BREAK THE "I BEFORE E" RULE.

CVE-2018-????? SKYLAKE x86 CHIPS CAN BE PRIED FROM THEIR SOCKETS USING CERTAIN FLATHEAD SCREWDRIVERS.

CVE-2018-????? APPARENTLY LINUS TORVALDS CAN BE BRIBED PRETTY EASILY.

CVE-2018-????? AN ATTACKER CAN EXECUTE MALICIOUS CODE ON THEIR OWN MACHINE AND NO ONE CAN STOP THEM.

CVE-2018-????? APPLE PRODUCTS EXECUTE ANY CODE PRINTED OVER A PHOTO OF A DOG WITH A SADDLE AND A BABY RIDING IT.

CVE-2018-????? UNDER RARE CIRCUMSTANCES, A FLAW IN SOME VERSIONS OF WINDOWS COULD ALLOW FLASH TO BE INSTALLED.

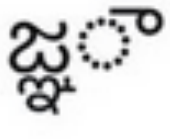
CVE-2018-????? TURNS OUT THE CLOUD IS JUST OTHER PEOPLE'S COMPUTERS.

CVE-2018-????? A FLAW IN MITRE'S CVE DATABASE ALLOWS ARBITRARY CODE INSERTION. [~~CLICK HERE FOR CHEAP VIAGRA~~]

Bugs

- Apple Telugu character bug
  https://twitter.com/steipete/status/963080391207931904?lang=en

  https://arstechnica.com/gadgets/2018/02/apple-releases-ios-11-2-6-and-macos-10-13-3-fixes-telugu-character-crash/



- Cisco Adaptive Security Appliance VPN bug
  https://arstechnica.com/information-technology/2018/01/cisco-drops-a-mega-vulnerability-alert-for-vpn-devices/

  https://arstechnica.com/information-technology/2018/02/that-mega-vulnerability-cisco-dropped-is-now-under-exploit/

- BitTorrent/uTorrent
  https://arstechnica.com/information-technology/2018/02/utorrent-bugs-let-websites-control-your-computer-and-steal-your-downloads/

30.72TB SSDs with 40GB caches

- https://www.anandtech.com/show/12448/samsung-begins-mass-production-of-pm1643-sas-ssds-with-3072-tb-capacity

- https://arstechnica.com/gadgets/2018/02/samsung-crams-30tb-of-ssd-into-a-single-2-5-inch-drive/

HomePod white ring of yuck

- https://thewirecutter.com/reviews/apple-homepod/
- https://www.macrumors.com/2018/02/15/pad-and-quill-homepod-coaster/

Be careful where you put it. The HomePod's base left rings on wood finishes. The rings faded over time, but we wouldn't risk it on good furniture. Photo: Jon Chase

http://appleinsider.com/articles/18/02/19/new-video-shows-drone-crashing-onto-roof-at-apple-park


Questions?