Security Now! #645 - 01-09-18

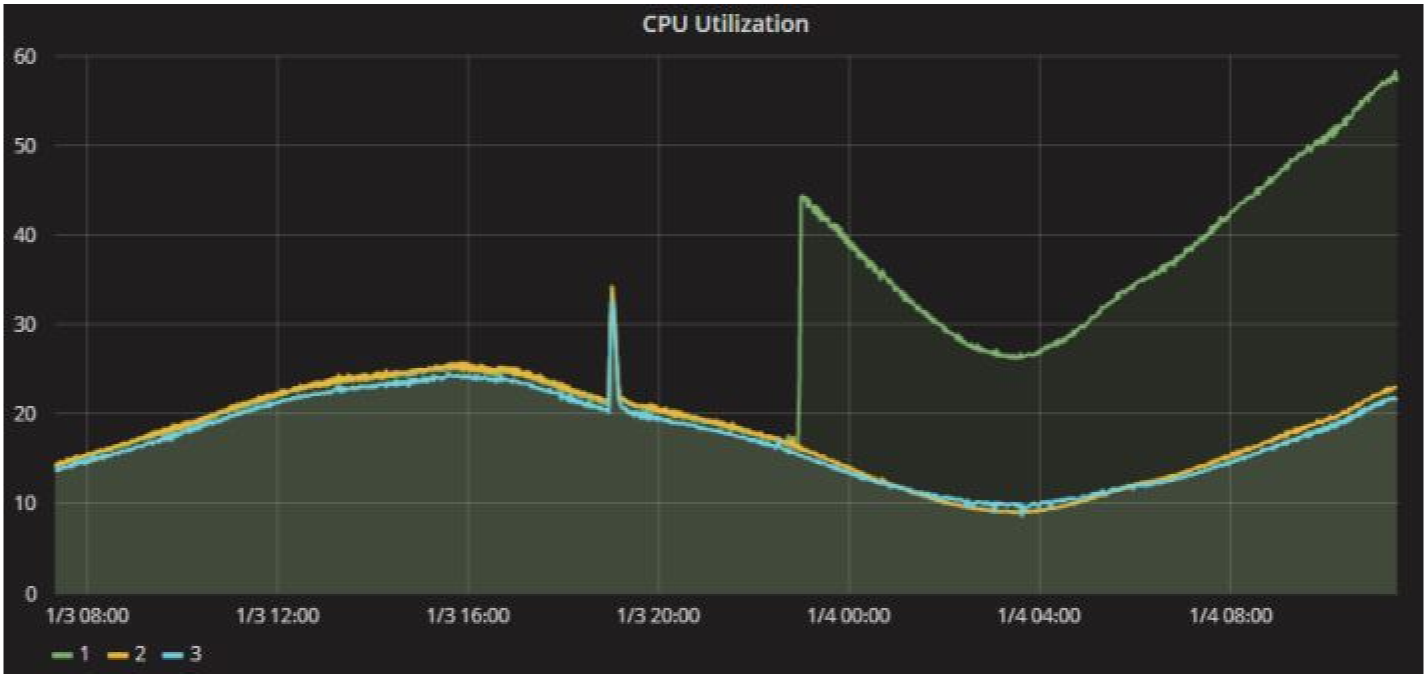
The Speculation Meltdown

This week on Security Now!

This week, before we focus upon the industry-wide catastrophe enabled by precisely timing the instruction execution of all contemporary high-performance processor architectures... we examine a change in Microsoft's policy regarding non-Microsoft A/V systems, Firefox Quantum's performance when tracking protections are enabled, the very worrisome hard-coding backdoors in ten of Western Digital's MyCloud drives, and if at first (WEP) and at second (WPA) and at third (WPA2) and at forth (WPS), you don't succeed... try, try, try try try yet again... with WPA3... another crucial cryptographic system being developed by a closed, members-only, committee.

The General Law of Cross-Task Information Leakage:
"In any setting where short-term performance optimizations have global effect, a sufficiently clever task can infer the recent history of other tasks by observing its own performance."

The consequence of Meltdown mitigation



"The following chart shows the significant impact on CPU usage of one of our back-end services after a host was patched to address the Meltdown vulnerability."
https://www.epicgames.com/fortnite/forums/news/announcements/132642-epic-services-stability-update

Security News

Microsoft:
"Important: Windows security updates released January 3, 2018 & antivirus software"
https://support.microsoft.com/en-us/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software

Overview

Microsoft has identified a compatibility issue with a small number of antivirus software products.

The compatibility issue arises when antivirus applications make unsupported calls into Windows kernel memory. These calls may cause stop errors (also known as blue screen errors) that make the device unable to boot. To help prevent stop errors that are caused by incompatible antivirus applications, Microsoft is only offering the Windows security updates that were released on January 3, 2018, to devices that are running antivirus software that is from partners who have confirmed that their software is compatible with the January 2018 Windows operating system security update.

If you have not been offered the security update, you may be running incompatible antivirus software, and you should consult the software vendor.

Microsoft is working closely with antivirus software partners to ensure that all customers receive the January Windows security updates as soon as possible.

More information

Windows Defender Antivirus, System Center Endpoint Protection, and Microsoft Security Essentials are compatible with the January 2018 security updates and have set the required registry key.

Windows 10, Windows 8.1, Windows Server 2012 R2 and Windows Server 2016 Customers
Microsoft recommends all customers protect their devices by running a compatible and supported antivirus program. Customers can take advantage of built-in antivirus protection, Windows Defender Antivirus, for Windows 8.1 and Windows 10 devices or a compatible third-party antivirus application. The antivirus software must set a registry key as described below in order to receive the January 2018 security updates.

Windows 7 SP1 and Windows Server 2008 R2 SP1 Customers
In a default installation of Windows 7 SP1 or Windows Server 2008 R2 SP1, customers will not have an antivirus application installed by default. In these situations, Microsoft recommends installing a compatible and supported antivirus application such as Microsoft Security Essentials or a third-party anti-virus application. The anti-virus software must set a registry key as described below in order to receive the January 2018 security updates.

Customers without Antivirus
In cases where customers can’t install or run antivirus software, Microsoft recommends manually setting the registry key as described below in order to receive the January 2018 security updates.

Setting the Registry Key

Caution Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing keys and values" help topic in Registry Editor (Regedit.exe) or view the "Add and delete information in the registry" and "Edit registry data" help topics in Regedt32.exe.

Note: Customers will not receive the January 2018 security updates (or any subsequent security updates) and will not be protected from security vulnerabilities unless their antivirus software vendor sets the following registry key:

```
Key="HKEY_LOCAL_MACHINE"
Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat"
Value="cadca5fe-87d3-4b96-b7fb-a231484277cc" Type="REG_DWORD”
Data="0x00000000”
```

Frequently asked questions

Q1: Why are some antivirus solutions incompatible with the January 3, 2018, security updates?

A1: During testing, we discovered that some third-party applications have been making unsupported calls into Windows kernel memory that cause stop errors (also known as bluescreen errors) to occur.
Microsoft has assembled the following resources to help potentially impacted customers:

- Troubleshoot blue screen errors in Windows 10
- Resolving Blue Screen errors in Windows 8.1
- Resolving stop (blue screen) errors in Windows 7

Q2: What is Microsoft doing to help mitigate issues caused by these unsupported applications?

A2: To help protect our customers from "blue screen" errors and unknown scenarios, Microsoft is requiring all antivirus software vendors to attest to the compatibility of their applications by setting a Windows registry key.

Q3: How long will Microsoft require setting a registry key to receive the January 3, 2018, security updates?

A3: Microsoft added this requirement to ensure customers can successfully install the January 2018 security updates. Microsoft will continue to enforce this requirement until there is high confidence that the majority of customers will not encounter device crashes after installing the security updates.

Q4: I have a compatible antivirus application but I’m not being offered the January 3, 2018, security updates. What do I do?

A4: In some cases, it may take time for security updates to be delivered to systems, particularly for devices that have been turned off or not connected to the Internet (offline). After they are turned on again, these systems should receive updates from their antivirus software providers. Customers who still experience problems 24 hours after ensuring that their devices have proper Internet connectivity should contact their antivirus software vendor for additional troubleshooting steps.

Q5: My antivirus software is not compatible. What should I do?

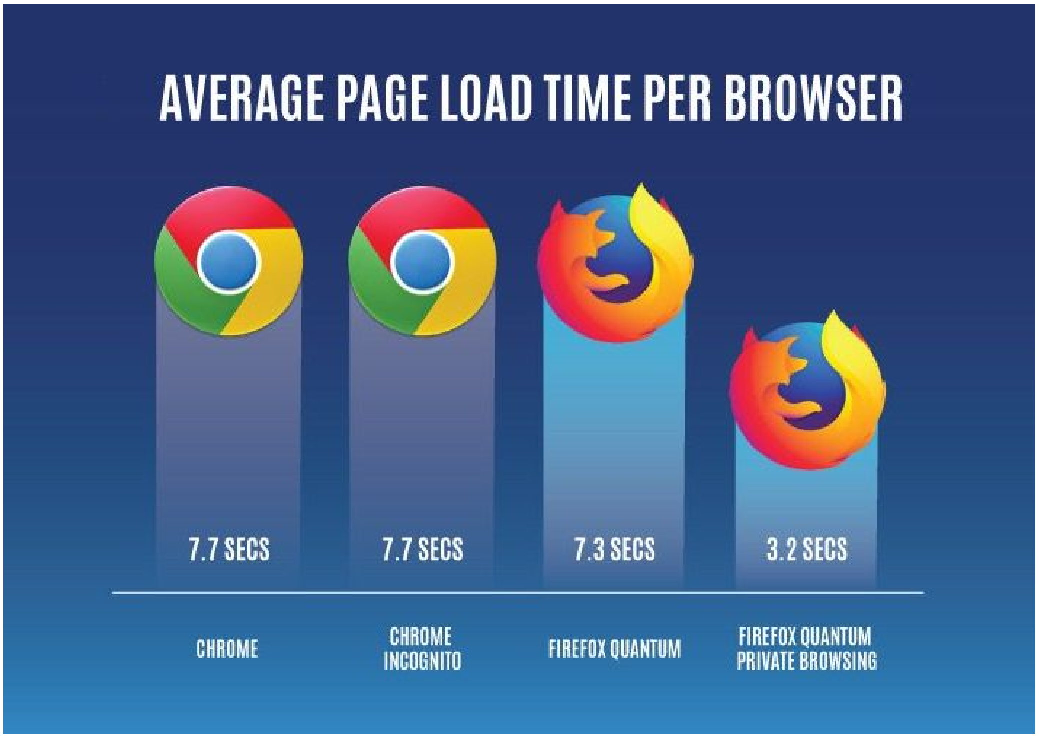
A5: Microsoft has been working closely with antivirus software partners to help all customers receive the January 2018 Windows security updates as soon as possible. If you are not being offered this month’s security update, Microsoft recommends that you contact your antivirus software provider.

Q6: I have a compatible antivirus software application, but I still experienced a bluescreen. What should I do?

A6: Microsoft has assembled the following resources to help potentially impacted customers:

- Troubleshoot blue screen errors in Windows 10
- Resolving Blue Screen errors in Windows 8.1
- Resolving stop (blue screen) errors in Windows 7

Jason Kint / @jason_kint
Seriously. Drop Chrome. Download latest version of @firefox (called Quantum) and turn on Tracking Protection in the settings. Tracking protection will also help mitigate ad fraud. And it's Google's Achilles heel.



Firefox Private Browsing vs. Chrome Incognito: Which is Faster?
https://blog.mozilla.org/blog/2017/11/20/firefox-private-browsing-vs-chrome-incognito/

"Most browser performance benchmarks focus on the use of a regular browsing mode. But, what about Private Browsing? Given that Private Browsing use is so common, we wanted to see how Firefox's Private Browsing compared with Chrome's Incognito when it came to page load time (that time between a click and the page being fully loaded on the screen)."

DuckDuckGo paper: https://duckduckgo.com/download/Private_Browsing.pdf

Results:

> Across the top 200 news websites tested, the average page load time for Firefox Quantum's Private Browsing is 3.2 seconds compared to Chrome's Incognito mode which took an average of 7.7 seconds to load a page for the fast Gigabit connection. This means that, on average, Firefox Quantum's Private Browsing loads page 2.4x faster than Chrome in Incognito mode.

The primary reason for the dramatic difference is that Mozilla's Private Browsing mode automatically activates Quantum' Tracking Protection, whereas Chrome's Incognito mode does not.

However, Firefox's Tracking Protection can be enabled 24/7 to give it an additional boost:

Mozilla writes:

> While the speed improvements in Firefox Quantum will vary depending on the website, overall users can expect that Private Browsing in Firefox will be faster than Chrome's Incognito mode right out of the box.
>
> In fact, due to these findings, we wanted users to be able to benefit from the increased speed and privacy outside of Private Browsing mode. With Firefox Quantum, users now have the ability to enable Tracking Protection in Firefox at any time.
>
> If you'd like to take it up a notch and enable Tracking Protection *every time* you use Firefox, then download Firefox Quantum, open Preferences. Choose Privacy & Security and scroll down until you find the Tracking Protection section. Alternatively, simply search for "Tracking Protection" in the *Find in Preferences* field. Enable Tracking Protection "Always" and you are set to enjoy both improved speed and privacy whenever you use Firefox Quantum.
>
> When enabling it, please keep in mind that Tracking Protection may block social "like" buttons, commenting tools and some cross-site video content.

Western Digital My Cloud drives had a hardcoded backdoor
https://www.techspot.com/news/72612-western-digital-cloud-drives-have-built-backdoor.html
https://www.bleepingcomputer.com/news/security/backdoor-account-removed-from-western-digital-nas-hard-drives/
http://www.securityweek.com/hardcoded-backdoor-found-western-digital-storage-devices
http://gulftech.org/advisories/WDMyCloud%20Multiple%20Vulnerabilities/125

James Bercegay, a security researcher with GulfTech Research and Development, discovered and reported these flaws to Western Digital back in June 2017. He then waited patiently for Western Digital to release firmware updates.

Three significant problems with the devices:

1) Unrestricted file upload - A PHP file found on the WD MyCloud's built-in web server allows an attacker to upload files on the device. Bercegay says he used this flaw to upload web shells to the device, which in turn granted him control over the device.

2) Hardcoded backdoor account - An attacker can log into vulnerable WD MyCloud NAS devices using the username "mydlinkBRionyg" and the password "abc12345cba". Bercegay says the backdoor doesn't give attackers admin access, but he was able to exploit another flaw and get root permissions for the backdoor account.

3) CSRF (Cross-Site Request Forgery) - A CSRF bug that can be exploited for executing rogue commands and pranks, such as changing the device's backend panel interface language.

In Mid-December an independent and highly detailed disclosure of the vulnerabilities was publicly posted: https://www.exploitee.rs/index.php/Western_Digital_MyCloud

Ten different WD MyCloud drives shared a common hardcoded backdoor. (My Cloud Gen 2, My Cloud EX2, My Cloud EX2 Ultra, My Cloud PR2100, My Cloud PR4100, My Cloud EX4, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100 and My Cloud DL4100.)

Logging in to Western Digital My Cloud services can be done by anybody using "mydlinkBRionyg" as the administrator username and "abc12345cba" as the password.

Bercegay says Western Digital released firmware version 2.30.174

Metasploit Module exists:
https://dl.packetstormsecurity.net/1801-exploits/GTSA_wdmycloud_backdoor.rb.txt

Description: This module exploits two issues. The first issue is that there is a hard coded backdoor within WDMyCloud devices. Using this backdoor access we can then reach buggy code which is vulnerable to command injection. A root shell will be spawned upon successful exploitation.

So be sure that you have the latest firmware installed into your WD MyCould drive.

How NOT to (ever) learn the lesson: Announce yet another Wi-Fi specification developed in secret: **Wi-Fi Alliance® introduces security enhancements**

> New Wi-Fi® security features available in 2018
>
> Las Vegas, NV – January 8, 2018 – Wi-Fi Alliance® introduces enhancements and new features for Wi-Fi Protected Access®, the essential family of Wi-Fi CERTIFIED™ security technologies for more than a decade. Wi-Fi Alliance is launching configuration, authentication, and encryption enhancements across its portfolio to ensure Wi-Fi CERTIFIED devices continue to implement state of the art security protections.
>
> WPA2™ provides reliable security used in billions of Wi-Fi® devices every day, and will continue to be deployed in Wi-Fi CERTIFIED devices for the foreseeable future. Wi-Fi Alliance will continue enhancing WPA2 to ensure it delivers strong security protections to Wi-Fi users as the security landscape evolves. Advanced Wi-Fi applications will rely on WPA2 with Protected Management Frames, broadly adopted in the current generation of Wi-Fi CERTIFIED devices, to maintain the resiliency of mission-critical networks. New testing enhancements will also reduce the potential for vulnerabilities due to network misconfiguration, and further safeguard managed networks with centralized authentication services.
>
> Building on the widespread adoption and success of WPA2, Wi-Fi Alliance will also deliver a suite of features to simplify Wi-Fi security configuration for users and service providers, while enhancing Wi-Fi network security protections. Four new capabilities for personal and enterprise Wi-Fi networks will emerge in 2018 as part of Wi-Fi CERTIFIED WPA3™. Two of the features will deliver robust protections even when users choose passwords that fall short of typical complexity recommendations, and will simplify the process of configuring security for devices that have limited or no display interface. Another feature will strengthen user privacy in open networks through individualized data encryption. Finally, a 192-bit security suite, aligned with the Commercial National Security Algorithm (CNSA) Suite from the Committee on National Security Systems, will further protect Wi-Fi networks with higher security requirements such as government, defense, and industrial.
>
> “Security is a foundation of Wi-Fi Alliance certification programs, and we are excited to introduce new features to the Wi-Fi CERTIFIED family of security solutions,” said Edgar Figueroa, president and CEO of Wi-Fi Alliance. “The Wi-Fi CERTIFIED designation means Wi-Fi devices meet the highest standards for interoperability and security protections.”

So, let's see…

- WEP(tm)... Hmmmmmm.
  Produced by the Wi-Fi Alliance and was nothing short of a massive embarrassment.
- WPA(tm) ... nope, better, but still readily hackable.
- WPS(tm) pushbutton configuration -- whoops, another disaster.
  Everyone urged to turn it off.
- WPA2(tm) ... more improvement, but they still didn't get it right.

The utter absurdity that something as important as secure wireless networking is being developed under the cover of darkness,via a closed process requiring expensive annual dues and membership should embarrass everyone involved in that ludicrous decades-old process.

2018's Plans for Lets Encrypt

https://letsencrypt.org/2017/12/07/looking-forward-to-2018.html

> Let’s Encrypt had a great year in 2017. We more than doubled the number of active (unexpired) certificates we service to 46 million, we just about tripled the number of unique domains we service to 61 million, and we did it all while maintaining a stellar security and compliance track record. Most importantly though, the Web went from 46% encrypted page loads to 67% according to statistics from Mozilla - a gain of 21 percentage points in a single year - incredible. We’re proud to have contributed to that, and we’d like to thank all of the other people and organizations who also worked hard to create a more secure and privacy-respecting Web.
>
> While we’re proud of what we accomplished in 2017, we are spending most of the final quarter of the year looking forward rather than back. As we wrap up our own planning process for 2018, I’d like to share some of our plans with you, including both the things we’re excited about and the challenges we’ll face. We’ll cover service growth, new features, infrastructure, and finances.

Yes, all true… but also a significant mixed blessing.

In 2018:

- Next version of their ACME protocol.
- Wildcard certificates
- Elliptic Curve (ECDSA) root to allow EC certificates.

SpinRite

David L in Utah
Subject: Thanks for giving me $728!!!!
Date: 19 Dec 2017 19:24:38

Steve and Leo,
I have been a Security Now listener since the single digits, but I didn't buy a copy of SpinRite until my computer wouldn't boot because of some error. Whatever it was, SpinRite fixed it. Thanks, Steve!

Also, thanks for $728! After your first episode about Bitcoin in 2009, I decided to download it and fiddled around for a week. My computer was too weak to mine, but I did go to a website called the Bitcoin Faucet, which gave me 5 Bitcoin Cents for free! I finally found my wallet in my backup drive, and I just sold them and netted $728. (By the way, it took my old computer two weeks to process the 157 GB block chain- which used to only be 250 MB when I got my 5 cents.)

Anyway, I must say it pays to listen to Security Now!

Closing The Loop

Mike Gatzke @mlgatzke
I’ve started using Firefox with the Tree Style Tab add-on. Is there a way for Firefox to remember the tabs I have open?
(Session Manager)

Richard J. Wilcox / @RichardJWilcox
@SGgrc @SimonZerafa I had the same experience as reported in this article.
The Microsoft update bricked my AMD Athlon 64 X2 6000+ computer.

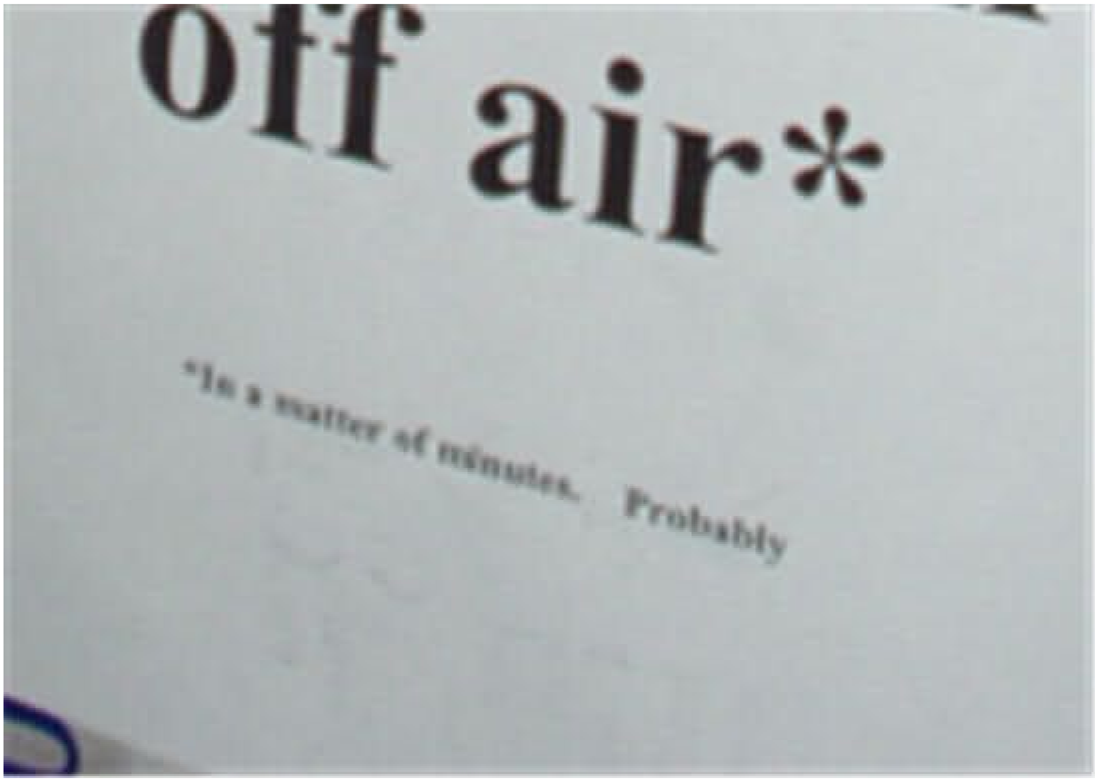
http://securityaffairs.co/wordpress/67498/hacking/microsoft-kb4056892-bricks-athlon-pcs.html
Older AMD Athlon and Sempron processors are experiencing troubles.
Posted to a Microsoft forum: "I have older AMD Athlon 64 X2 6000+, Asus MB, after installation of KB4056892 the system doesn't boot, it only shows the Windows logo without animation and nothing more. After several failed boots it do roll-back then it shows error 0x800f0845. Unfortunately, it seems it's not easy to disable the automatic updates without gpedit tweaks, so it tries installing and rolling-back the update over and over. The sfc /scannow shows no problem, in-place upgrade also doesn't seem to help. I can try full reinstall, but I doubt it will change anything. It seems like the update is binary incompatible with my old CPU. I understand that making the machine unbootable is the best protection from remote exploitation, but I would rather have the OS working."

"Same issue here, but with an AMD Sempron 3200+ processor and 32-bit Win10 Pro. I had to do a reset to fix...."

Woody Leonhard / @woodyleonhard
Replying to @SimonZerafa @SGgrc @explanoit
I'm getting reports of a LOT of AMD Win7 machines blue screening, plus a handful of others - Intel, Win10, various mixtures. No common theme as yet except Win7 AMD Athlons really took a hit.

Johnny Brian / @johnnybrian
@SGgrc I have an older Mac Pro as my main computer. The latest OS it can run is 10.11.6. It’s not clear if Apple will patch this OS for Meltdown - support.apple.com/en-us/HT208331. Should I be concerned? Replacement is not an option. Should I disconnect it from the internet?

Via Twitter:
@SGgrc @leolaporte Re: SN#644 Picture of the week: I believe the small text on the UKTV fan notice says "*In a matter of minutes. Probably". This appears to be the original source:
http://thedailywtf.com/articles/Sophisticated-Cooling-Apparatus



Ian Beckett @ianbecket
@SGgrc I'm wondering how vunerable #ARM controllers in SSD's are to #spectre #meltdown and the like ? - #cybersecurity

Andres Vidal @andresvidal
@GibsonResearch I just read that MongoDB noticed a 10-15% impact on HVM hypervisors from patches applied to their AWS infrastructure. That seems really high! CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754

Trevor Welch @TWelch333
@SGgrc @leolaporte Is there any reason why Security now is not on Spotify but other TWIT shows are? Trying to consolidate my podcasts into a nice cross-platform (including fire stick) app and would love to see it on there.

The Speculation Meltdown

The General Law of Cross-Task Information Leakage:
"In any setting where short-term performance optimizations have global effect, a sufficiently clever task can infer the recent history of other tasks by observing its own performance."

Finally we have a problem that it's probably not possible to over-hype.

FOUR different unrelated groups all reported these problems to Intel within the span of two months. Wired Magazine's coverage of this made what I think is an extremely interesting observation: Under the heading of "Quadruple Collision", writing for Wired, Andy Greenberg wrote: "In fact, the bizarre confluence of so many disparate researchers making the same discovery of two-decade-old vulnerabilities raises the question of who else might have found the attacks before them—and who might have secretly used them for spying, potentially for years, before this week's revelations and the flood of software fixes from practically every major tech firm that have rushed to contain the threat.
https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/?mbid=social_twitter_onsiteshare

Project Zero
https://googleprojectzero.blogspot.hr/2018/01/reading-privileged-memory-with-side.html
https://meltdownattack.com/meltdown.pdf
https://spectreattack.com/spectre.pdf

Intel CEO: Meltdown and Spectre patches will come to 90%+ of chips in the next week
https://techcrunch.com/2018/01/08/intel-ces/
With the microchip processing industry facing perhaps its biggest security scare in its history, the CEO of one of the world's biggest chipmakers, Brian Krzanich of Intel, took to the stage at a keynote at CES to say a few words about the news before launching into his planned announcements covering areas like automotive, AI and entertainment.

"I want to thank the industry for coming together to address the recent security, industry-wide issue. Security is job number one for Intel and our industry," he said. "The primary focus for us has to keep our customer data safe."

He said that Intel had not received any information that any data has been compromised on its chips to date. "We are working tirelessly to make sure it stays that way," he added.

He also said that Intel expects to issue updates to its processors soon. More than 90 percent will be getting them within the week, and the rest by the end of January.

Intel facing class-action lawsuits over Meltdown and Spectre bugs
https://www.theguardian.com/technology/2018/jan/05/intel-class-action-lawsuits-meltdown-spectre-bugs-computer

Speculation... What is it?

Speculative execution is a technique used by high speed processors in order to increase performance by guessing likely future execution paths and prematurely executing the instructions in them. For example when the program's control flow depends on an uncached value located in the physical memory, it may take several hundred clock cycles before the value becomes known. Rather than wasting these cycles by idling, the processor guesses the direction of control flow, saves a checkpoint of its register state, and proceeds to speculatively execute the program on the guessed path. When the value eventually arrives from memory the processor checks the correctness of its initial guess. If the guess was wrong, the processor discards the (incorrect) speculative execution by reverting the register state back to the stored checkpoint, resulting in performance comparable to idling. In case the guess was correct, however, the speculative execution results are committed, yielding a significant performance gain as useful work was accomplished during the delay.

From a security perspective, speculative execution involves executing a program in possibly incorrect ways. However, as processors are designed to revert the results of an incorrect speculative execution on their prior state to maintain correctness, these errors were previously assumed not to have any security implications.

Intel's Plans:
https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Intel-Analysis-of-Speculative-Execution-Side-Channels.pdf

3.2 - Branch Target Injection Mitigation

For the branch target injection method, two mitigation techniques have been developed. This allows a software ecosystem to select the approach that works for their security, performance and compatibility goals.

The first technique introduces a new interface between the processor and system software. This interface provides mechanisms that allow system software to prevent an attacker from controlling the victim's indirect branch predictions, such as flushing the indirect branch predictors at the appropriate time to mitigate such attacks. This details of this interface will be provided in a future revision of the Intel®64 and IA-32 Architectures Software Developer's Manuals. This mitigation strategy requires both updated system software as well as a microcode update to be loaded to support the new interface for many existing processors. This new interface will also be supported on future Intel processors. There are three new capabilities that will now be supported for this mitigation strategy. These capabilities will be available on modern existing products if the appropriate microcode update is applied, as well as on future products, where the performance cost of these mitigations will be improved.

What's Old is New Again...
1995: "The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems."
https://pdfs.semanticscholar.org/2209/42809262c17b6631c0f6536c91aaf7756857.pdf
1995: on page 9 under section "4.2 Security Flaws": Item 6. Prefetching may fetch otherwise inaccessible instructions in Virtual 8086 mode. (From a paper in 1992!) -- 25 years ago.

Speculation Control Validation PowerShell Script
https://gallery.technet.microsoft.com/scriptcenter/Speculation-Control-e36f0050

A small and clean utility on Github:
https://github.com/ionescu007/SpecuCheck
https://github.com/ionescu007/SpecuCheck/releases/
https://github.com/ionescu007/SpecuCheck/releases/tag/1.0.4

Posted by Raspberry Pi Founder Eben Upton...
https://www.raspberrypi.org/blog/why-raspberry-pi-isnt-vulnerable-to-spectre-or-meltdown/
Why Raspberry Pi isn't vulnerable to Spectre or Meltdown
(Their ARM core doesn't speculate -- doubtless less expensive to license and much smaller die area.)