DATA INSECURITY:

How One of the Worst Computer Defects Ever Sacrificed Security for Speed

October 2019

NCL
NATIONAL CONSUMERS LEAGUE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In January 2018, it was announced that researchers had discovered some of the most significant cyber security vulnerabilities the public has ever faced. The vulnerabilities, which stem from serious flaws found in central processing units (CPUs), also known as processors or chips, leave nearly every computer, server and other device from the last 20 years susceptible to hacking.

Researchers in the academic community and from companies like Google discovered the vulnerabilities and described them as "probably one of the worst CPU bugs ever found,"[1] with news reports around the world noting how they would "make nearly any computer vulnerable to hacking"[2] and "just as bad as you think."[3]

"[Meltdown] is probably one of the worst CPU bugs ever found."

– Daniel Gruss, one of the researchers at Graz University of Technology who discovered the flaw[4]

The first exploit to be discovered, called "Spectre," affects practically every CPU on the planet such as those manufactured by AMD, ARM and Intel. At the same time, another exploit, "Meltdown", was announced alongside Spectre but is largely specific to Intel processors – the chipmaker for the vast majority of computers and servers used by consumers and businesses around the world.

But that was not the end of the story. Since that January 2018 announcement, an additional five Intel-specific exploits – with names such as "Foreshadow" and "Zombieload" – have been disclosed, and experts believe even more will be discovered. Due to the nature of the flaws, attacks that take advantage of these exploits may not be traceable.

While it is not uncommon for bugs and security gaps to be found in computers, they traditionally are quickly patched with software updates and never thought of again. However, these vulnerabilities are fundamentally different as they affect the hardware, and specifically the brains, of nearly every computer and server around the world. Given that the flaws are foundational to how the CPU is built and each patch is only temporary until the next exploit is discovered, the threat to consumers and the institutions they interact with daily remains.

While software patches have been released to address these issues, consumers often do not install all security updates. To make things worse, for those consumers who have installed the patches, the updates can slow their computers and servers - in some cases up to 40 percent - while performing certain tasks.

Consumers' only foolproof solution for these flaws is to replace the device with a new one that has been reengineered to fix the issue and restore the security and performance they were guaranteed – an option that may be unaffordable and out of reach for many consumers. Until then, consumers are in the untenable position of having to decide between speed or security.

The National Consumers League as part of its #DataInsecurity Project[6] has engaged with cybersecurity and technology experts and reviewed hundreds of research papers, news articles, and online discussions so consumers can fully understand the impact of these processor flaws. In the pages that follow, we discuss the threat these flaws pose to consumers – both in terms of the security of their data and the performance of their computers – and how they can protect themselves in the future.

"This is the most significant security news we've had in the last 10 years. Some of the mitigations are going to be extremely expensive. I think this is the real deal."

– Avi Rubin, computer science professor at Johns Hopkins University specializing in health-care security[5]

---

[1]Samuel Gibbs, "Meltdown and Spectre: 'Worst Ever' CPU Bugs Affect Virtually All Computers," *The Guardian*, January 4, 2018, https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw

[2]Andrew Griffin, "Intel Chip Flaw: Huge Bug Makes Nearly Any Computer Vulnerable to Hacking," *The Independent*, January 4, 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/intel-chip-flaw-hacking-computer-security-hackers-cyber-crime-amd-arm-a8141106.html

[3]Matthew Hughes, "Spectre and Meltdown are just as bad as you think," *The Next Web*, January 4, 2018, https://thenextweb.com/security/2018/01/04/spectre-and-meltdown-are-as-bad-as-you-think/

[4]Daniel Gruss et al., "Meltdown: Reading Kernel Memory from User Space," *meltdownattack.com*, January 2, 2018, https://meltdownattack.com/meltdown.pdf

[5]Elizabeth Dwoskin, Hamza Shaban, and Craig Timberg, "Huge Security Flaws Revealed – and Tech Companies Can Barely Keep Up," *The Washington Post*, January 5, 2018, https://www.washingtonpost.com/business/technology/huge-security-flaws-revealed--and-tech-companies-can-barely-keep-up/2018/01/05/82ccbe18-f24e-11e7-b3bf-ab90a706e175_story.html

[6]"NCL Data Insecurity Project," National Consumers League, accessed October 1, 2019, https://www.nclnet.org/datainsecurity

DATA BREACHES REGULARLY ENDANGER CONSUMERS

Data breaches happen with frightening regularity. Capital One recently lost the personal information of more than 100 million people in one of the largest-ever thefts of data from a bank.[7] In 2018, it was Marriott who lost 500 million records[8] and Under Armour who lost 150 million.[9] The year before Equifax lost 145 million records.[10] These are just the major breaches that captured worldwide headlines. Smaller incursions and ransomware attacks targeting individual consumers, businesses, and governments occur on a daily basis.

A multitude of harms can occur when a consumer's sensitive data is stolen, including, but not limited to, identify theft, fraud, credit and reputational harm, erroneous tax claims and extortion. According to the Insurance Information Institute, in 2017 there was a record high of 16.7 million victims of identity fraud.[11] Global computer security software company McAfee and the Center for Strategic and International Studies (CSIS) estimated the likely annual cost to the global economy from cybercrime is $600 billion a year.[12] In just the first half of 2019, over 4.1 billion records were exposed from nearly 4,000 data breaches, according to the 2019 MidYear Data Breach QuickView Report.[13] In fact, the number of reported data breaches was up 54 percent from last year.

Given these staggering numbers, it is clear that most consumers have probably been affected in one way or another by an IT security related event – either on their personal computer or through an organization or business that they have entrusted with their sensitive information.

On an individual level, the threat from a data breach can range from a minor nuisance to life changing. It can mean financial loss, the inconvenience of freezing a credit card and requesting a new one, disputing unwanted charges, unnecessary hits to credit scores or, in more nefarious cases, fighting instances of a stolen identity or fraud. In the end, the growing number of data breaches and their serious repercussions may ultimately lead to less trust in the marketplace by consumers.

The CPU flaws discussed here amplify the data breach problem. In addition to creating another avenue for hackers to pursue access to sensitive data, these vulnerabilities are likely to persist for years because they are hardware-based. Software patches designed to address the flaws do not fully resolve the problem. In many cases, they create additional challenges associated with a computer's speed and performance. Just as important, hacks targeting these vulnerabilities are untraceable and are extremely well known in the hacker community. In fact, there are easily accessible videos online that demonstrate exactly how to exploit these vulnerabilities.[14]

---

[7]Rob McLean, "A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts," *CNN*, July 30, 2019, https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

[8]Zack Whittaker, "Marriott Says 500 Million Starwood Guest Records Stolen in Massive Data Breach," *TechCrunch*, November 30, 2018, https://techcrunch.com/2018/11/30/starwood-hotels-says-500-million-guest-records-stolen-in-massive-data-breach/

[9]Maria Armental and Sara Germano, "Under Armour Discloses Breach Affecting 150 Million MyFitnessPal App Users," *The Wall Street Journal*, March 29, 2018, https://www.wsj.com/articles/under-armour-discloses-breach-affecting-150-million-myfitnesspal-app-users-1522362412

[10]Brian Fung, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," *The Washington Post*, May 8, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/

[11]"Facts and Statistics: Identity Theft and Cybercrime," Insurance Information Institute, accessed October 1, 2019, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[12]James Andrew Lewis, "Economic Impact of Cybercrime," Center for Strategic and International Studies, September 19, 2019, https://www.csis.org/analysis/economic-impact-cybercrime

[13]"2019 MidYear QuickView Data Breach Report," Risk Based Security, accessed October 1, 2019, https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[14]"Hacking Livestream #43: Meltdown and Spectre," January 24, 2018, https://www.youtube.com/watch?v=0o6MoJ2gHHI

THE DEFECTS INSIDE NEARLY EVERY COMPUTER

A central processing unit is the brain where the calculations that run a computer are performed.[15] While CPUs were first developed in the middle of the last century and have evolved greatly since then, their general premise remains the same: they carry out all of a computer's tasks via the instructions it is given by a particular software program. Computer processors are supposed to carry out these instructions in a way that is secure – preventing access to confidential information as it runs through the system.

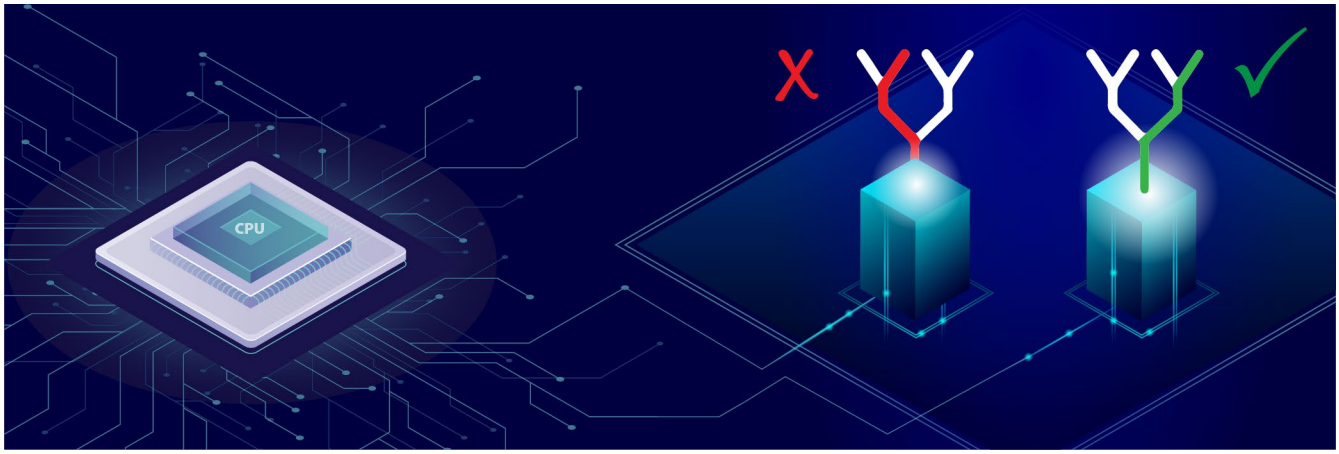
But it turns out this confidential information in the processor may not be as secure as we once believed. In January 2018, researchers from the academic community and companies like Google announced the discovery of security exploits "Spectre"[16] and "Meltdown."[17] News outlets across the globe reported on this development as one of the greatest computer security threats ever discovered with major consequences for every consumer and business.[18, 19]

As previously mentioned, unlike most computer security issues which can be easily patched with software updates, these exist at the hardware level and impact millions of computers produced over the last two decades.[20]

"If you have an issue in hardware, it's not very easy to just change the hardware because you already sold millions of CPUs. And you just can't call them back and change them."

– Moritz Lipp, researcher at Graz University of Technology[21]

Because Spectre and Meltdown were announced on the same day, and by nature are very technical, it led to confusion as to who was impacted and the severity of the problem. But in the nearly two years that have passed since their discovery, the impact on consumers have become clearer and more frightening.



Using speculative execution, a processor can predict, or speculate, a user's next action and perform it in advance – increasing the speed of the computer.

[15] Jonathan Strickland, "What's Inside My Computer?" *HowStuffWorks*, September 23, 2008, https://computer.howstuffworks.com/inside-computer1.htm
[16] Daniel Gruss *et al.*, "Spectre" https://spectreattack.com
[17] Daniel Gruss *et al.*, "Meltdown" https://meltdownattack.com
[18] Peter Bright, "'Meltdown' and 'Spectre:' Every Modern Processor has Unfixable Security Flaws," *Ars Technica*, January 4, 2018, https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws/
[19] Douglas Busvine and Stephen Nellis, "Security flaws put virtually all phones, computers at risk," *Reuters*, January 3, 2018, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO
[20] Andy Greenberg, "A Critical Intel Flaw Breaks Basic Security for Most Computers," *Wired*, January 3, 2018, https://www.wired.com/story/critical-intel-flaw-breaks-basic-security-for-most-computers/
[21] Scott Neuman, "Apple: Mac and iOS Vulnerable to meltdown and Spectre Flaws," *NPR*, January 5, 2018, https://www.npr.org/sections/thetwo-way/2018/01/05/575867249/apple-mac-and-ios-vulnerable-to-meltdown-and-spectre-flaws

Both exploits involve a technology called "speculative execution"[22] that was introduced in the 1990s by Intel and other chipmakers in their pursuit of ever-faster processors. This functionality allows modern CPUs to "speculate" or guess what process a user is going to run next, thereby increasing the speed and performance of the processor by preventing the delays that would be incurred by doing the work after instructions are given.

Spectre affects all modern processors, such as those manufactured by AMD, ARM, Intel and even the processor inside your Android or iPhone cell phone. Spectre breaks down the walls between different applications and allows attackers to trick programs into leaking their secrets. Thankfully, Spectre is very difficult for a hacker to exploit according to experts.[23]

On the other hand, Meltdown is derived from a separate flaw that is largely specific to Intel processors. Researchers believe it is much easier for hackers to exploit. The name refers to the fact that "[t]he vulnerability basically melts security boundaries which are normally enforced by the hardware."[24] In short, it allows an unauthorized user to access privileged information.

Researchers believe that the problem stems from how Intel designed its processors, which are found in the vast majority of computers and servers used by consumers and businesses today,[25] and implemented its version of speculative execution. According to *The Register*, the publication which broke the news of the defects, "Intel's CPUs speculatively execute code potentially without performing security checks. Researchers believe that it may be possible to craft software in such a way that the processor starts executing an instruction that would normally be blocked – such as reading kernel memory from user mode – and completes that instruction before the privilege level check occurs."[26]

Since Meltdown was discovered, five additional attacks (Foreshadow[27], Zombieload[28], RIDL[29], Fallout[30] and SWAPGS[31]) were discovered which are all specific to the flaw found in Intel processors. And as each attack has been discovered and security updates issued, researchers immediately demonstrated that these patches can hamper a computer's performance.[32]

	Spectre[16] (Announced Jan. 2018)	Meltdown[17] (Announced Jan. 2018)	Foreshadow[27] (Announced Aug. 2018)	Zombieload[28] (Announced May 2019)	RIDL[29] (Announced May 2019)	Fallout[30] (Announced May 2019)	SWAPGS[31] (Announced Aug. 2019)
AMD	✓						
ARM	✓	— Only one processor affected (Cortex A-75)[33]					
Intel	✓	✓	✓	✓	✓	✓	✓

Since January 2018, seven exploits have been publicly disclosed that take advantage of processor flaws related to speculative execution. While Spectre affected major chip manufacturers AMD, ARM, and Intel all subsequent exploits have largely affected only Intel chips.

[22] Joel Hruska, "What is Speculative Execution?" *ExtremeTech*, May 16, 2019, https://www.extremetech.com/computing/261792-what-is-speculative-execution
[23] Brian X. Chen and Cade Metz, "What You Need to Do Because of Flaws in Computer Chips," *The New York Times*, January 4, 2019, https://www.nytimes.com/2018/01/04/technology/meltdown-spectre-questions.html
[24] Gruss *et al.*, "Meltdown."
[25] Khaveen Jeyaratnam, "Intel Vs. AMD: Battle For Market Share," *Seeking Alpha*, March 11, 2019, https://seekingalpha.com/article/4247790-intel-vs-amd-battle-market-share
[26] Chris Williams, "Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign," *The Register*, January 2, 2018, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/
[27] "The Foreshadow Attack," accessed October 1, 2019, https://foreshadowattack.eu/
[28] "The Zombieload Attack," accessed October 1, 2019, https://zombieloadattack.com/
[29] "RIDL and Fallout: MDS attacks," accessed October 1, 2019, https://mdsattacks.com/
[30] "RIDL and Fallout."
[31] "SWAPGS," accessed October 1, 2019. https://www.swapgs.com/
[32] Joel Hruska, "Intel Performance Hit 5x Harder Than AMD After Spectre, Meltdown Patches," *ExtremeTech*, May 20, 2019, https://www.extremetech.com/computing/291649-intel-performance-amd-spectre-meltdown-mds-patches
[33] "Vulnerability of Speculative Processors to Cache Timing Side-Channel Mechanism," *armDeveloper*, June 17, 2019, https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability

CONSUMERS' CRITICAL DATA AT RISK

Consumers' data is stored by a multitude of companies that use online data centers, otherwise known as cloud computing. These companies rely upon servers that are built with these flawed CPUs and are vulnerable to these exploits unless patched and secured.

Practically every computer and server in the world is subject to Spectre and requires updates to mitigate the threat. Devices with Intel chips, which power the vast majority of the world's computer infrastructure, have needed ongoing updates[34] to bolster security and address the problem because they are vulnerable to all seven exploits.

The impact to consumers stretches far beyond their personal computers. Major companies that consumers rely upon use servers that are built with these flawed CPUs and are vulnerable to these exploits.[35] These servers contain countless sensitive records and information that, if compromised, have severe consequences. U.S. government officials – including members of Congress, the National Security Agency and the Department of Homeland Security – have expressed concerns regarding the national security implications of these flaws and how these vulnerabilities came to light.[36]

"The delays in notification and in some cases just the complete lack of notification was a big mistake,"

– Sen. John Thune (R-SD)[37]

"It's been reported that Intel informed Chinese companies of the Spectre and Meltdown vulnerabilities before notifying the U.S. government. As a result, it's highly likely that the Chinese government knew about the vulnerabilities."

– Sen. Bill Nelson (D-FL)[38]

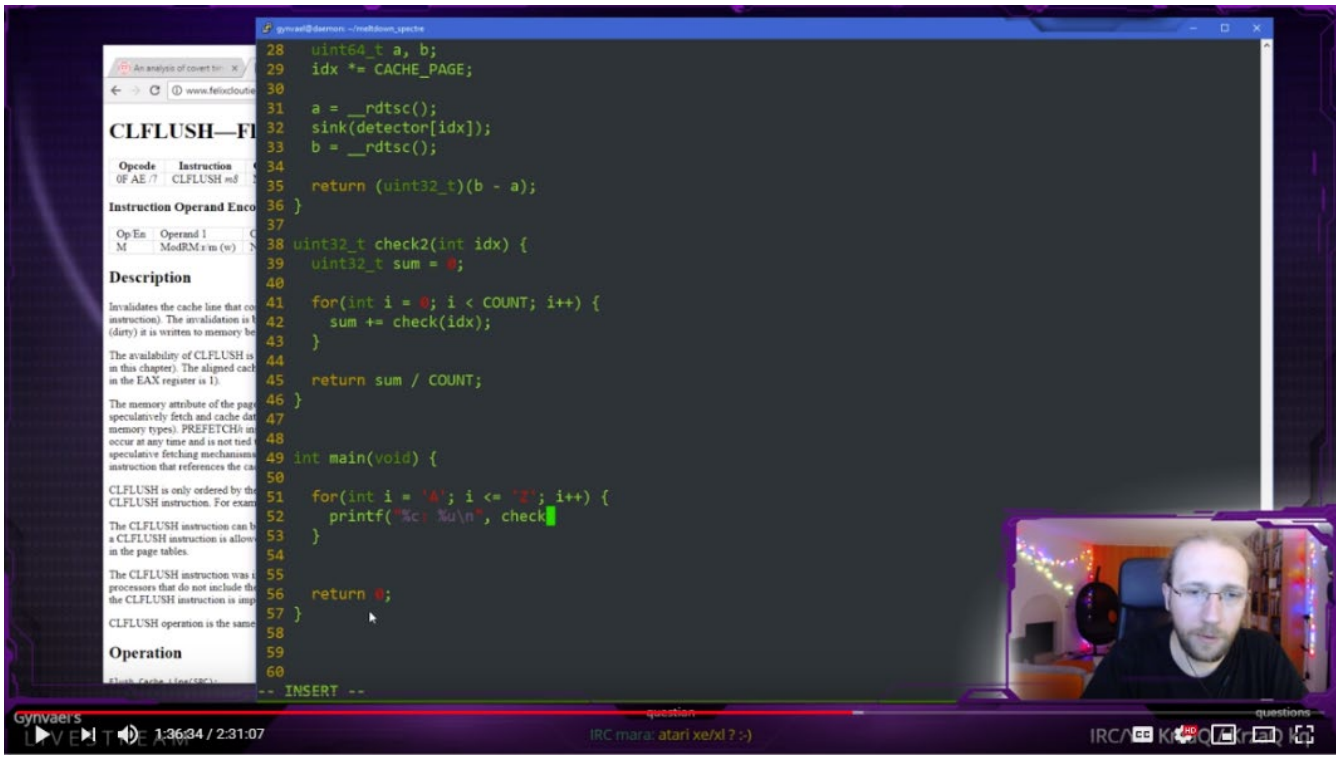
[34]Dan Meyer, "Constant Updates Key to Fighting Spectre, Meltdown, Foreshadow," *SDX Central*, August 30, 2018, https://www.sdxcentral.com/articles/news/constant-updates-key-to-fighting-spectre-meltdown-foreshadow/2018/08/
[35]Cade Metz and Nicole Perlroth, "Researchers Discover Two major Flaws in the World's Computers," *The New York Times*, January 3, 2018, https://www.nytimes.com/2018/01/03/business/computer-flaws.html
[36]Lily Hay Newman, "Senators Fear Meltdown and Spectre Disclosure Gave China an Edge," *Wired*, July 11, 2018, https://www.wired.com/story/meltdown-and-spectre-intel-china-disclosure/
[37]Sean Lyngaas, "Senators question vulnerability disclosure process after Spectre and meltdown stumbles," *Cyberscoop*, July 11, 2018, https://www.cyberscoop.com/senators-question-vulnerability-disclosure-process-spectre-meltdown-stumbles/
[38]Newman, "Senators Fear."

To take advantage of these processor defects, for example, hackers could rent space on a cloud service and use these exploits to obtain information that another business had on the same server – such as passwords or customers' credit card details.[39] In the event that a hacker did exploit these vulnerabilities, consumers may not be aware it occurred until it was too late. When hackers take advantage of these vulnerabilities, they leave no trace.[40]

These vulnerabilities are well known in the hacker community. In fact, there are even videos available online depicting actual white-hat hackers (individuals with the skills to hack into a computer but do so solely to advise individuals and companies) breaking into computer systems via these vulnerabilities.[41] These vulnerabilities are not theoretical or a secret – the instruction manuals are public and easily accessible.

"Exploits for these bugs will be added to hackers' standard toolkits."

– Dan Guido, chief executive of cybersecurity consulting firm Trail of Bits[42]



This video by Gynvael Coldwind, an IT security engineer at Google, shows exactly how a hacker could exploit these vulnerabilities and steal sensitive information, without leaving a trace.

[39] Gibbs, "Meltdown and Spectre."
[40] Gruss *et al.*, "Meltdown."
[41] "Hacking Livestream #43: Meltdown and Spectre."
[42] Gibbs, "Meltdown and Spectre."

THE PATCHES: A CHOICE BETWEEN SECURITY AND PERFORMANCE

"For now, computer owners and data center operators will have to make an unsavory choice: Use Intel's software patches and accept slower speeds, or skip the patches and remain at risk."

– Bloomberg[43]

While the performance impact of these vulnerabilities depends on a variety of factors, such as the age and generation of the processor, the operating system being used, the type of work being conducted and other factors, this much is clear: the patches and mitigations that help to secure your computer can slow it down to a concerning degree. What makes this more problematic for consumers is that older Intel devices running older operating systems – which make up a significant segment of the consumer market[44] – are impacted the most.[45]

A brand-new computer may not experience the same performance impacts that a two- or five-year-old computer would. However, because many consumers do not upgrade their computers often, the security vulnerability tied to these flaws can linger. As former Intel CEO Brian Krzanich noted, "[The] replacement cycle for the PC has extended. Four years was the average, now it has moved to about five to six years."[46]

"It makes you shudder. The processor people were looking at performance and not looking at security."

– Paul Kocher , computer security expert[47]

Microsoft has stated, for example, that Windows 7 users, which according to NetMarketShare encompasses approximately 36 percent of the desktop and laptop market, and Windows 8/8.1 users, which is another five percent of the market, will "notice a decrease in system performance" when using computers with Intel processors over several generations. Even Windows 10 users, with approximately 44 percent of the market, may experience a performance hit.[48]

Each patch compounds the performance impact of previous patches. While the collective impact of enabling all patches varies on an application-by-application level, some industry websites have calculated the collective decrease of performance to be 15 to 16 percent on all Intel CPUs without hyper-threading disabled.[49]

What Is Hyper-Threading?

Hyper-threading is Intel's term for simultaneous multithreading (SMT), which increases a CPU's performance by improving its efficiency, thereby allowing you to run multiple demanding apps at the same time without the PC lagging.[50]

However, some of the most recent vulnerabilities (Zombieload, RIDL, Fallout) can only be mitigated by disabling hyper-threading. For example, Apple provides the option to enable "full mitigation" which provides protection from these security issues, but the update may reduce performance by up to 40 percent.[51] Google disabled hyper-threading on its Chrome operating system by default, noting, "some users may notice slower performance with some apps and games."[52]

The software patches could slow the performance of affected machines by 20 to 30 percent, said Andres Freund, an independent software developer who has tested the new Linux code. The researchers who discovered the flaws voiced similar concerns. This could become a significant issue for any business running websites and other software through cloud systems.[53]

Consumers are now left in the unenviable position of needing to choose between security and the performance they anticipated. As NCL has long advocated, security must be prioritized – despite the speed consequences that consumers may, however unfairly and wrongly, need to bear as a result.

---

[43]Max Chafkin and Ian King, "Intel Has a Big Problem. It Needs to Act Like It," *Bloomberg*, January 18, 2018, https://www.bloomberg.com/news/features/2018-01-18/intel-has-a-big-problem-it-needs-to-act-like-it
[44]"Operating System Share by Version," Net Market Share, accessed October 14, 2019.
[45]Gordon Mah Ung, "Here's how much the Meltdown and Spectre patches drag down older hardware," *PCWorld*, January 24, 2018, https://www.pcworld.com/article/3250645/how-meltdown-and-spectre-patches-drag-down-older-hardware.html
[46]Agam Shah, "The PC Upgrade Cycle Slows to Every Five to Six Years, Intel's CEO Says," *PCWorld*, June 1, 2016, https://www.pcworld.com/article/3078010/the-pc-upgrade-cycle-slows-to-every-five-to-six-years-intels-ceo-says.html
[47]Ian King et al., "'It Can't Be True.' Inside the Chip Industry's Meltdown," *Bloomberg*, January 8, 2018, https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown
[48]Terry Myerson, "Understanding the Performance Impact of Spectre and Meltdown Mitigations on Windows Systems," *Microsoft Security*, January 9, 2018, https://www.microsoft.com/security/blog/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/
[49]Michael Larabel, "The Performance Impact Of MDS / Zombieload Plus The Overall Cost Now Of Spectre/Meltdown/L1TF/MDS," *Phoronix*, May 18, 2019, https://www.phoronix.com/scan.php?page=article&item=mds-zombieload-mit&num=1
[50]"Get Faster Performance For Many Demanding Business Applications," Intel, accessed October 1, 2019, https://www.intel.com/content/www/us/en/architecture-and-technology/hyper-threading/hyper-threading-technology.html?
[51]"Additional mitigations for speculative execution vulnerabilities in Intel CPUs," Apple, accessed October 1, 2019, https://support.apple.com/en-us/HT210107
[52]"Change your Chromebook's performance setting," Google Support, accessed October 1, 2019, https://support.google.com/chromebook/answer/9340236?hl=en
[53]Metz and Perlroth, "Researchers Discover."

THE IMPACT

"[Intel] makes about 90 percent of the world's computer processors and 99 percent of the server chips in the data centers that effectively run the internet."

– Bloomberg[54]

The defects impact nearly every computer on the planet, and are fully integrated into the hardware design of affected CPUs.[55] In turn, consumers are now left to play whack-a-mole to protect their information, as new patches are regularly required, with unclear impacts on their computer from both a security and speed standpoint. Exploits taking advantage of the flaws will likely continue to evolve. This in turn will place a continuous burden upon consumers to keep their computers secure.

In addition, patches and mitigations, while necessary, undermine performance not just for consumers' personal computers but also on the cloud computing services that consumers rely on. Organizations or individuals running large-scale, heavy workloads, like virtualization and data center/cloud workloads, on their servers have seen a significant performance impact. For example, Epic Games, which runs the popular online video game Fortnite, showed a roughly 20 percent increase in CPU utilization immediately after the patches were applied.[56]

"The biggest cost to businesses is just going to be the lifecycle of all the hardware that we previously assumed we can use for two [to] six years or more. It is now going to end its lifecycle sooner because it's not going to be as powerful."

– Dan Alig, chief information officer of Wharton Computing and Information Technology[57]

The financial costs of implementing the patches and addressing each vulnerability derived from the defects could also become a burden for consumers. Businesses now have to account for, and pass on to consumers, the added cost of:

- Acquiring new servers without the flawed CPUs, meaning unplanned or early hardware upgrade cycles;
- Acquiring additional servers to handle the same amount of work in order to offset the reduced capacity from patch implementation;
- Purchasing additional energy to power the additional servers; and
- Appropriating manpower and resources to track and confront the exploits.[58, 59]

Additional costs are further magnified for consumers when considering the small businesses they interact with are likely to be running "legacy" hardware or software. These businesses may not be able to afford the high cost of additional servers to offset the speed loss from the patches, hiring or redeploying staff to deal with the vulnerabilities, and/or entirely replacing old systems. This difficult choice for small businesses could mean that some decide against applying patches – with potentially severe consequences for consumers' data security.

---

[54]Chafkin and King, "Intel."
[55]Lindsey O'Donnell, "Intel ZombieLoad Side-Channel Attack: 10 Takeaways," *Threat Post*, May 15, 2019, https://threatpost.com/intel-zombieload-side-channel-attack-10-takeaways/144771/
[56]Tom Warren, "Epic Games Blames Meltdown CPU Performance Issues for Fortnite Downtime," *The Verge*, January 6, 2018, https://www.theverge.com/2018/1/6/16857878/meltdown-cpu-performance-issues-epic-games-fortnite
[57]Mike Chapple and Andrea Matwyshyn, "How Spectre and Meltdown Will Impact Companies and Consumers," *Knowledge@Wharton Podcast*, January 23, 2018, https://knowledge.wharton.upenn.edu/article/spectre-and-meltdown/
[58]Maria Korolov, "Spectre, Meltdown Hit On-Prem Windows Servers Hardest," *Data Center Knowledge*, January 23, 2018, https://www.datacenterknowledge.com/security/spectre-meltdown-hit-prem-windows-servers-hardest
[59]Chapple and Matwyshyn, "How Spectre."

WHAT CONSUMERS CAN DO

5 Things Consumers Can Do
1 **Be prepared.** Make sure you have all systems set to automatically update, which can help ensure your devices have the latest and most secure software.
2 **Stay in the know.** New exploits continue to be announced, so it's best to track the news and install the appropriate updates and patches, despite the potential performance impacts.
3 **Remain up to date.** In addition to installing the more regular patches and updates that become available, running the latest operating system can also create a more secure system. For Windows, this means Windows 10; the latest version of macOS is called Catalina.
4 **Protect yourself.** If you're purchasing a new computer or device, it may be best to purchase one that has hardware-level fixes and is not affected by the performance issues that comes with patches. If purchasing a refurbished computer, be sure to wipe the hard drive and install the operating system from scratch with all updates that are available.
5 **Take action.** Ask your Congressional representative to support data security bills like the Consumer Privacy Protection Act of 2017, which would require companies to take preventive steps to defend against cyberattacks.

The best protection for consumers is to buy a new computer that has hardware-level security fixes that also do not have the performance issues associated with some of the patches. Of course, this is not practical for many consumers who expect to use their computer for years before upgrading. In a new white paper, Intel has proposed a new type of memory that if implemented could provide better protection against the attacks – which shows that these flaws are in fact addressable at the hardware level.[60]

That being said, there are steps consumers can take with their current devices. The first step is awareness. We advise consumers to remain vigilant in tracking the latest exploits and installing the appropriate updates and patches – despite the potential speed and performance impacts. We also continue to advise that consumers take the appropriate data hygiene measures to ensure that their data is as secure as possible. This includes avoiding phishing emails, creating diverse and complex passwords, utilizing two factor authentication, and being sure to update antivirus software regularly.

An easy step for consumers to take is to ensure their systems have updates set to automatically install. There is often a reflexive nature to hit the "ignore" or "later" button when asked whether to install updates. However, these updates contain important security patches that are critical for protecting your data. Having automatic updates in place can help ensure your computer or mobile device is more secure.

Second, consumers should update to the latest operating system, assuming their computer or device supports it. For Windows, this means Windows 10, and the latest version of Mac OS (known as Catalina).

As it relates to these exploits, to help consumers sort through the dizzying array of patches and mitigations, Intel has provided a resource and response page.[61] Other vendors such as Microsoft[62] and Apple[63] have similar pages. Those considering a refurbished computer with an affected processor that has known vulnerabilities should understand the security issues uncovered to date. Because

[60] Catalin Cimpanu, "Intel proposes new SAPM memory type to protect against Spectre-like attacks," *ZDNet*, October 1, 2019, https://www.zdnet.com/article/intel-proposes-new-sapm-memory-type-to-protect-against-spectre-like-attacks/
[61] "Resources and Response to Side Channel Variants 1, 2, 3," Intel, August 10, 2018, https://www.intel.com/content/www/us/en/architecture-and-technology/side-channel-variants-1-2-3.html
[62] "Windows Server guidance to protect against speculative execution side-channel vulnerabilities," Microsoft Security, May 14, 2019, https://support.microsoft.com/en-us/help/4072698/windows-server-speculative-execution-side-channel-vulnerabilities-prot
[63] "About speculative execution vulnerabilities in ARM-based and Intel CPUs," Apple, accessed October 1, 2019, https://support.apple.com/en-us/HT208394

Spectre impacts practically all consumer-grade processors, that exploit is unavoidable. However, those purchasing a refurbished computer should ensure all security patches are applied, and depending on how they plan to use the computer, account for possible speed and performance impacts.

"The costs alone are insane," said Tony Cole, vice president and global government chief technology officer at FireEye. He estimated that a global overhaul would amount to trillions of dollars in new expenses. "It would be mind-boggling if everyone tried."

– The Washington Post[64]

Another major issue is whether to turn off Intel's hyperthreading in order to help thwart certain exploits that take advantage of its flaws. As stated earlier, Google has disabled it by default on Chromebooks, while Microsoft[65] and Apple[66] have not but do provide instructions on how to do so. Turning off hyperthreading can provide fuller protection against the Fallout, RIDL, and ZombieLoad exploits, but the performance impact is so substantial (as much as 40 percent according to Apple). This decision should not be made lightly (versus applying software updates, which NCL recommends installing by default).

Finally, consumers can ask their representatives in Congress to support data security bills like the Consumer Privacy Protection Act of 2017.[67] This bill would require companies to take preventive steps to defend against cyberattacks and data breaches, and to quickly provide consumers with notice and appropriate protection when a data breach occurs. Senator Patrick Leahy, who wrote the bill, stated "companies that profit from our personal information should be obligated to take steps to keep it safe, and to provide notice and protection to consumers when those protections have failed." This can also be extended to the companies that create the hardware that processes and stores this sensitive data. Consumers have a right to data security and data privacy, and Congress must take action accordingly to protect them.

---

[64]Craig Timberg, Elizabeth Dwoskin, and Hamza Shaban, "Huge security flaws revealed — and tech companies can barely keep up," *The Washington Post*, June 5, 2018, https://www.washingtonpost.com/business/technology/huge-security-flaws-revealed--and-tech-companies-can-barely-keep-up/2018/01/05/82ccbe18-f24e-11e7-b3bf-ab90a706e175_story.html

[65]Microsoft Security, "Windows Server guidance."

[66]"How to enable full mitigation for Microarchitectural Data Sampling (MDS) vulnerabilities," Apple, https://support.apple.com/en-us/HT210108

[67]U.S. Congress, Senate. Consumer Privacy Protection Act of 2017. S. 2124, 115th Cong. Introduced in Senate November 14, 2017.

CONCLUSION

Cybersecurity bugs and exploits that directly impact consumers come and go; patches are issued, without any noticeable difference in how our computers operate. But what makes these processor exploits so dangerous is their ubiquity and the fact that patching them results in a real trade-off – reduced performance – that could lead consumers and businesses to choose speed over security. Since Spectre and Meltdown were announced in January 2018, the fact that five additional exploits have been discovered – largely affecting Intel processors that are used by the vast majority of consumers – means these flaws will continue to be a threat for the foreseeable future.

When consumers buy new technology, there is an expectation that they will receive the speed and performance they were promised, as well as security. The idea of trading one for the other is not a consideration that would enter anyone's mind when buying a computer which is used regularly to store and process sensitive information.

The flaws create a real challenge for consumers: apply each temporary "fix" as new exploits are discovered and risk slowing down your device, or don't and put your sensitive information at risk. Consumers are at the mercy of companies that hold their sensitive data who are faced with a similar dilemma, particularly as they must consider the expenses of implementing these fixes – including costs to add computing power lost by each patch.

At some point, all of the systems in place today will be replaced with new processors that have been redesigned at the hardware level to fix the flaws and thwart these exploits. Intel has stated that they expect all future processors will include hardware mitigations addressing these vulnerabilities.[68] In the meantime consumers will be forced to choose between the speed they were promised and security.

Ultimately, for those who continue to be impacted today, it's likely safer to be slower than sorry.

[68] "Side Channel Vulnerability Microarchitectural Data Sampling," Intel, accessed October 1, 2019, https://www.intel.com/content/www/us/en/architecture-and-technology/mds.html

ABOUT NCL

For confidence and safety in the marketplace and workplace since 1899.

The National Consumers League is America's pioneering consumer advocacy organization, representing consumers and workers on marketplace and workplace issues since our founding in 1899. Headquartered in Washington, DC, today NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including child labor, privacy, food safety, and medication information.

NCL's #DataInsecurity Project has a two-pronged mission to both educate consumers and policymakers on how to protect themselves from data breaches and cyber-attacks. Likewise, the #DataInsecuirty project also advocates before Congress and industry to urge them to act immediately to protect consumers' data. The #Datainseructy project urges policymakers to:

· Create a national data breach notification standard, modeled on strong state protections such as California's;

· Require businesses that maintain consumers' personal data to protect that information via specific data security requirements;

· Grant the Federal Trade Commission and state Attorneys General civil penalty authority to enforce violations of data security requirements;

· Increase civil and criminal penalties for malicious hacking;

· Increase efforts to enhance cooperation with international partners to bring overseas hackers to justice; and

· Require retailers and banks to implement the highest level of security available to protect consumers' payment data.

· Allow consumers to control their data whether it is collected by a company, via an app, or data that was gathered by a vehicle.

For more information on this report, contact:

John Breyault
Vice President, Public Policy Telecommunications and Fraud
National Consumers League
1701 K Street, NW Ste 1200
Washington, DC 20006

Email: johnb@nclnet.org | Phone: (202) 835-3323 | @ncl_tweets