What Users Must Know About Meltdown and Spectre Flaws Impacting CPUs

Briefly: Meltdown and Spectre are two vulnerabilities that impact almost all computers, tablets and smartphones. Does it mean you can be hacked? What can you do about it?

Meltdown and Spectre: What Really Matters

If you haven't heard, there is a bit of panic going on right now. No one knows whether or not computers around the world are secure.

Last week, we finally learned about Meltdown and Spectre. Two gaping security flaws found in almost every device on the planet.

We're basically just one bad hack away from disaster. All because one key component, our processors, have a glaring oversight. If you know how to ask the machine correctly they'll just give away our passwords,

The fault lies in a process known as 'speculative execution', a function that attempts to predict inputs ahead of time to speed things up and improve the computers overall performance.

But now we know this feature has a problem, as *Gizmodo* explains:

'*…there's a serious flaw in the way modern processors are hardcoded to use speculative execution - they don't check permissions correctly and leak information about speculative commands that don't end up being run. Whoops.*'

Whoops is right. It means your personal data is at serious risk. Because once they've got your password they can get access to details like credit cards, bank accounts, identification and more.

Even antivirus software may not save you. Spectre can be loaded into JavaScript, a coding language for the web, meaning it's up to your web browser to protect against the threat.

Luckily most web browser developers are on top of things. Google Chrome, Firefox, Internet Explorer, Microsoft Edge and Safari have all received updates, although some fixes are still being fleshed out for some browses

Fortunately there have been no known incidents as of yet. But that doesn't mean we can rest easy. Especially the people who make the chips.

Is it catastrophic?

The key thing to remember is not to panic, as the sky isn't about to come crashing down.

While these flaws impact a huge number of devices, there have been no widespread attacks so far. This is because it's not straightforward to get the sensitive data from the kernel memory. It's a possibility but not a certainty. but now that these flaws have been made public, the odds tick up that hackers will try to exploit them.

While Meltdown and Spectre are serious, a majority of organisations (and users for that matter) will only need to apply patches as normal and follow their usual patching policies. The situation is one that centres on information disclosure, not code execution (a far more troubling issue to deal with). There is a stronger sense of urgency if the organisation is in a unique situation (e.g. cloud providers, government contractors, finance), but that's a case-by-case assessment.

Perhaps you might have already heard about these flaws and are concerned about how you might be affected. I am going to summarise them here so that you would know the essentials of these vulnerabilities, their impacts and how you can you protect yourselves.

First, what are these flaws?

Meltdown

Basically, all computer processes occur in what are essentially sealed rooms which are supposed to be inaccessible to other processes. Meltdown takes advantage of a design flaw to allow other processes to access the kernel's private memory areas. This memory can contain the secrets (including passwords) of other programs and the operating system, and is supposed to be 'out of bounds' to unauthorized access by other apps. Think of it as as similar to a country's highly restricted command and control centre. What has happened is not unlike the 'top brass' unwittingly allowing the janitor's master key to give access to the innermost sanctum or leaving a copy of sensitive documents in the waiting room.

This makes your system vulnerable to attacks where a malicious program (even a JavaScript running on a website) can try to find the passwords from other programs in the kernel's private memory zone.

This vulnerability is exclusive to Intel CPUs and it can be exploited on shared cloud systems. Thankfully, it can be patched by system updates. Microsoft, Linux, Google and Apple have already started to provide fixes.

Spectre

Spectre also deals with kernel memory but in a slightly different way. This vulnerability actually allows a malicious program to trick another process running on the same system to leak its private information.
This vulnerability impacts Intel, AMD and ARM devices. This also means that the chips used in smartphones and tablets are also at risk.
Spectre is hard to patch but it is hard to exploit as well. Discussions are ongoing to provide a workaround through a software patch.

How to protect your computer from Meltdown and Spectre?

Practically every modern processor is vulnerable because that's where the major fault is.

1 - Hardware

Get an UEFI/BIOS Update for Your PC
Because these vulnerabilities are primarily and inextricably linked to your computer's CPU, there's only so much that software can do to mitigate the threats. To be fully effective, you'll need to get an UEFI firmware or BIOS update from your PC's manufacturer. This is not a project for the faint-hearted, so if the thought gives you horripilations then you should ask Peter Daley to help you.

2 – Software

How to Protect Yourself From Meltdown

Linux

Major Linux distros have Meltdown patches,

Android phones

According to Google, a new security update dated Jan. 5 will include "mitigations" to help protect your phone, and future updates will include more such fixes.
If you've got a Google-branded phone, such as a Nexus 5X or Nexus 6P, there's not a lot you need to do -- at some point your phone should automatically download the update, and you'll simply need to install it. With the Pixel and Pixel 2 (and their XL variants) it's even easier -- it'll automatically install, too.
Theoretically, the same goes for other Android phones, but many manufacturers and cellular carriers can be a little slow to issue patches. You may want to poke your phone's manufacturer and cellular carrier (particularly in public places) to ensure they update in a timely fashion. Squeaky wheels get the grease.
If you have an older phone you may be out of luck.

iPhones and iPads (and iPod touch)

If you've already installed the latest iOS version 11.2 on your iPhone or iPad, you should already be protected from some of the vulnerabilities that researchers discovered as of last month. Apple says that version, released on Dec. 2, included a number of mitigations, and Apple's promising to develop more protections in future updates.
To check, go to **Settings > General > About** and look for **Version** to verify you're on 11.2 or later. If not, go to **Settings > General > Software Update** to download the latest version.

Windows PCs

Microsoft has released a rare, out-of-band emergency patch for Windows 10 users. It should pop up and ask you to restart your machine so it can be installed, but if you have yet to receive such a notification, then head to **Settings > Update & security** see if there are updates waiting on the Windows Update page. If you are running Windows 10 version 1709 (Fall Creators Update), the patch you need is labeled **Security Update for Windows (KB4056892)**.
For older versions of Windows 10, here are the patch numbers:

- Windows 10 version 1703 (Creators Update): KB4056891
- Windows 10 version 1607 (Anniversary Update): KB4056890
- Windows 10 version 1511 (November Update): KB4056888
- Windows 10 version 1507 (Initial Release): KB4056893

Manual install route

If you have yet to receive the patch via Windows Update, you can manually install it by going to this Windows Update Catalog page. Odds are you are running a 64-bit version of Windows, so you'll

want to install the file for x64-based systems. For Fall Creators Update, for example, it's the bottom-most option labeled "2018-01 Cumulative Update for Windows 10 Version 1709 for x64-based Systems (KB4056892)."

Warning - No more Windows patches at all if your AV clashes with our Meltdown fix

Your antivirus must be compatible with Microsoft's Meltdown-Spectre fixes for you to get patches this month or in future.

As Microsoft warned this week, it's not delivering its January 3 Windows security updates to customers if they're running third-party antivirus, unless the AV is confirmed to be compatible with it.

Microsoft won't let you install future security updates until your antivirus vendor sets a specific registry key that certifies compatibility with Windows.

As part of this week's security updates for the Meltdown and Spectre CPU attacks, Microsoft required that all third-party antivirus vendors confirm compatibility with its CPU fixes and then to set a registry key in their products to certify compatibility. Without the key being set, Microsoft's security update simply won't install.

Microsoft has now clarified that this new rule will apply to all future security updates and means users running non-conforming third-party antivirus won't be protected by Microsoft's future patches.

How can you be sure you're protected?

To check to see if you have installed the necessary patch, go to **Settings > Update & security** and click **View installed update history**. Under **Quality Updates**, look to see that **Security Update for Windows (KB4056892)** was successfully installed. You can also check by going to **Settings > System > About** and scrolling down to the **Windows specifications** section. After installing the KB4056892 patch, the **OS Build** will read **16299.125**.

What else can you do?

So far, there have been no known attacks using the Meltdown or Spectre vulnerabilities, but now that these flaws have been made public, the odds tick up that hackers will try to exploit them. After updating your system and checking for a firmware update, you should run a scan using your AV app to check for any malicious software. And keep your apps updated, most notably your browser, and, as always, beware of dodgy web sites and phishing emails that can give hackers access to your machine.

Will the Meltdown fix slow down your computer?

The short answer to this question is 'possibly'. If you use an Intel CPU, you may notice a drop in performance after you apply the software update for Meltdown. In fact, several researchers claim that Intel deliberately kept the vulnerability open in order to get the slight performance boost over its competitor AMD.

How to Protect Yourself From Spectre

While you can protect yourself from Meltdown, it's harder to defend against the more invasive Spectre flaw. According to researchers involved in discovering and reporting on the two exploits, software updates to patch particular flaws in Spectre are possible, although none are able to address the exploit completely without a redesign of the operating system and the microprocessor itself. "It is important to note that this method (of attack) is dependent on malware running locally, which means it's imperative for users to practice good security hygiene by keeping their software up-to-date and avoiding suspicious links or downloads," AMD said in a statement.

How Hackers Can Read Your Websites' Passwords Using Meltdown And Spectre [With Solution]

Several recently-published research articles have demonstrated a new class of timing attacks (Meltdown and Spectre) that work on modern CPUs. Experiments confirm that it is possible to use similar techniques from Web content to read private information between different origins.

The first question is whether you're vulnerable or not. Most probably, Yes. The flaws are in all modern CPUs so you're most likely affected by it.

Secondly, how can an attacker can read your system's memory? Web content (Javascript code etc.) can read private information of a website visitor. Attackers may also start compromising websites to run the malicious code on the visitors' device to read sensitive information such as passwords saved in a web browser. The upshot is that users (like us) who mostly surf Internet on their devices are insecure. All it needs is a visit to a malicious website.

After the disclosure of the vulnerabilities by Google security blog, all software vendors came out and said that they had been working on a fix since they were informed.
Firefox and Chrome have also confirmed that they're working on a patch. Chrome will release a Meltdown protected version soon. So will Chrome users have to wait that long? Yes, but there is also a quick solution.

Firefox

Mozilla has just released an updated version of Firefox browser that includes fixes for the Meltdown and Spectre bugs discovered in Intel, AMD, and ARM processors.
The new version is Firefox 57.0.4 and it doesn't include any other change, as Mozilla prioritised patches for the two vulnerabilities in this release.

Chrome

Google this week issued Chrome 63 for Windows, macOS and Linux, adding important security enhancements including site isolation.

Enable Site Isolation To Protect Browsers Against Meltdown And Spectre

Besides waiting for Chrome to release the Meltdown protected version, Chrome/Chromium users can also use the solution that is already there. It's called Site Isolation. In chrome or Chromium (also Slimjet), users can enable site isolation. By enabling Site Isolation, the content of every website is always rendered in a dedicated process and isolated from other websites. It makes the content not readable for other websites. In case you visit a malicious website which runs code on your browser, it won't be able to see data of other websites.
To enable Site Isolation in Chrome/Chromium, copy the following URL in URL bar -

chrome://flags/#enable-site-per-process

Now you can see the highlighted option is Strict site isolation. Enable it. Now you're done. Restart your web browser and the site isolation is working.
NB! This also works in Slimjet (a chrome-based alternative browser without Googles inquisitiveness).

Site Isolation For Firefox Users

The only solution for Firefox seems to be First-Party Isolation. First-Party Isolation separates cookies and makes then inaccessible to other websites so it may not work against these vulnerabilities. It's uncertain if it separates the entire website content from other websites. First-Party Isolation is not enabled by default in Firefox right now. One reason for that may be that the feature may interfere with the authentication system on some sites. Try it out to see if that is the case on your end. If it gives you trouble, you can easily disable it at any time to restore the status quo.

1. Load the URL about:config?filter=privacy.firstparty.isolate in the Firefox address bar and and accept the risk. Or type about:config in the address bar and and accept the risk, then search for privacy.firstparty.isolate
2. Double-click on privacy.firstparty.isolate to set the preference to true.

This is all that needs to be done.
NB! There is also the Firefox add-on First Party Isolation which you can install instead. It does the same thing, but comes with an option to disable the functionality temporarily. It does require the latest firefox (at least version 58.0a1). https://addons.mozilla.org/en-US/firefox/addon/first-party-isolation/

How to Stop the Meltdown and Spectre Patches from Slowing Down Your PC

The Windows patches for Meltdown and Spectre will slow your PC down. On a newer PC running Windows 10, you probably won't notice. But, on a PC with an older processor—especially if it's running Windows 7 or 8—you may see a noticeable slowdown. Here's how to make sure your PC performs as speedily as possible after securing it. Whatever you do, please don't avoid installing the patches. The Meltdown and Spectre attacks are bad—very bad. Windows, macOS, Linux, Android, iOS, and Chrome OS are all being patched to correct the problem. Intel has also pledged that they'll be working with software companies to reduce the performance impact over time. But these are big security holes that you should absolutely patch. That doesn't mean you have to deal with the slowdown, however.
Upgrade to Windows 10 (If You're Using Windows 7 or 8)
There's no getting around it: The patch performs better if you're using Windows 10. As Microsoft puts it, on "2015-era PCs with Haswell or [an] older CPU", they "expect that some users will notice a decrease in system performance". But, with Windows 7 or 8 on the same older hardware, they "expect most users to notice a decrease in system performance."

In other words, on the same hardware, Microsoft says most people will notice a slowdown on Windows 7 or 8, while most people won't on Windows 10. As Microsoft explains: "Older versions of Windows have a larger performance impact because Windows 7 and Windows 8 have more user-kernel transitions because of legacy design decisions, such as all font rendering taking place in the kernel." Windows 10 is much newer software, and has many optimizations that the older Windows 7 and 8 just don't have.

Microsoft is talking about Intel CPUs, but there may be some slowdown when using AMD CPUs, too. The Meltdown fix doesn't apply to AMD systems, but the Spectre fix does. We haven't seen any performance benchmarks from AMD systems yet, so we don't know how performance has changed.

Rather than avoiding or disabling the patch, just upgrade to Windows 10. While the first year free upgrade period is technically over, there are still ways to get Windows 10 for free.

If you're not a fan of Windows 10, there are ways to make it less annoying. You can gain more control over Windows 10's automatic updates or just set your "Active Hours" so they don't bother you. You can hide all those obnoxious ads in Windows 10 and make it look more like Windows 7, if you like. You never even have to touch the Windows Store—you can just keep using the desktop and have a modern Windows operating system that performs faster than Windows 7.

Upgrade Your Hardware

Modern PCs—that is, "2016-era PCs with Skylake, Kabylake or a newer CPU"—perform better with the patch than older PCs. In fact, Microsoft says that "benchmarks show single-digit slowdowns, but we don't expect most users to notice a change because these percentages are reflected in milliseconds." That's because these Intel CPUs have a PCID (Process-Context Identifiers) feature that help the patch perform better. Without this feature, more of the work has to be done in software, and that slows things down. If you're curious whether your system has the feature that speeds up the patch, we recommend you download and run the Gibson Research Corporation's InSpectre tool. It will also tell you whether your PC is protected against Meltdown and Spectre or not.

If you see "Performance: GOOD", you have a modern PC with the appropriate hardware features and you shouldn't see a noticeable slowdown. If you don't, you have an older PC and you may see some extra lag. (Though remember, you can speed things up noticeably by upgrading to Windows 10, if you haven't already.)

If you feel your Windows 7 or 8 system is noticeably slower, the best thing you can do is to upgrade to Windows 10. Meltdown and Spectre are very serious security flaws that could potentially be exploited by code running on a web page in your web browser. You really don't want to use a vulnerable system.

Is your PC vulnerable to Meltdown and Spectre CPU exploits? InSpectre tells you

The vital information you need to know about the serious Meltdown and Spectre CPU exploits isn't whether your PC is inherently vulnerable to them—it is—but whether your system has been patched to protect against the flaws. Finding that information isn't easy though. You need to sift through update logs, cross-referencing them with arcane vulnerability identifiers and Microsoft Knowledge Base codes—or at least you *did*. Gibson Research recently released InSpectre, a wonderfully named, dead simple tool that detects if your PC is vulnerable to Meltdown and Spectre. InSpectre is a small program that doesn't need a formal install and scans your computer for Meltdown and Spectre susceptibility in mere milliseconds. When it's done, the program pops up with clear, easy-to-read information about the security status of your system. Scrolling down reveals a more in-depth explanation of your PC's security situation, once again using no-nonsense language to help you understand what's protected and what's not. Much like Gibson's other software, InSpectre *just works*. This is the sort of software Microsoft or Intel should have released to help clarify the murky, convoluted patching situation around this devastating duo of CPU exploits.