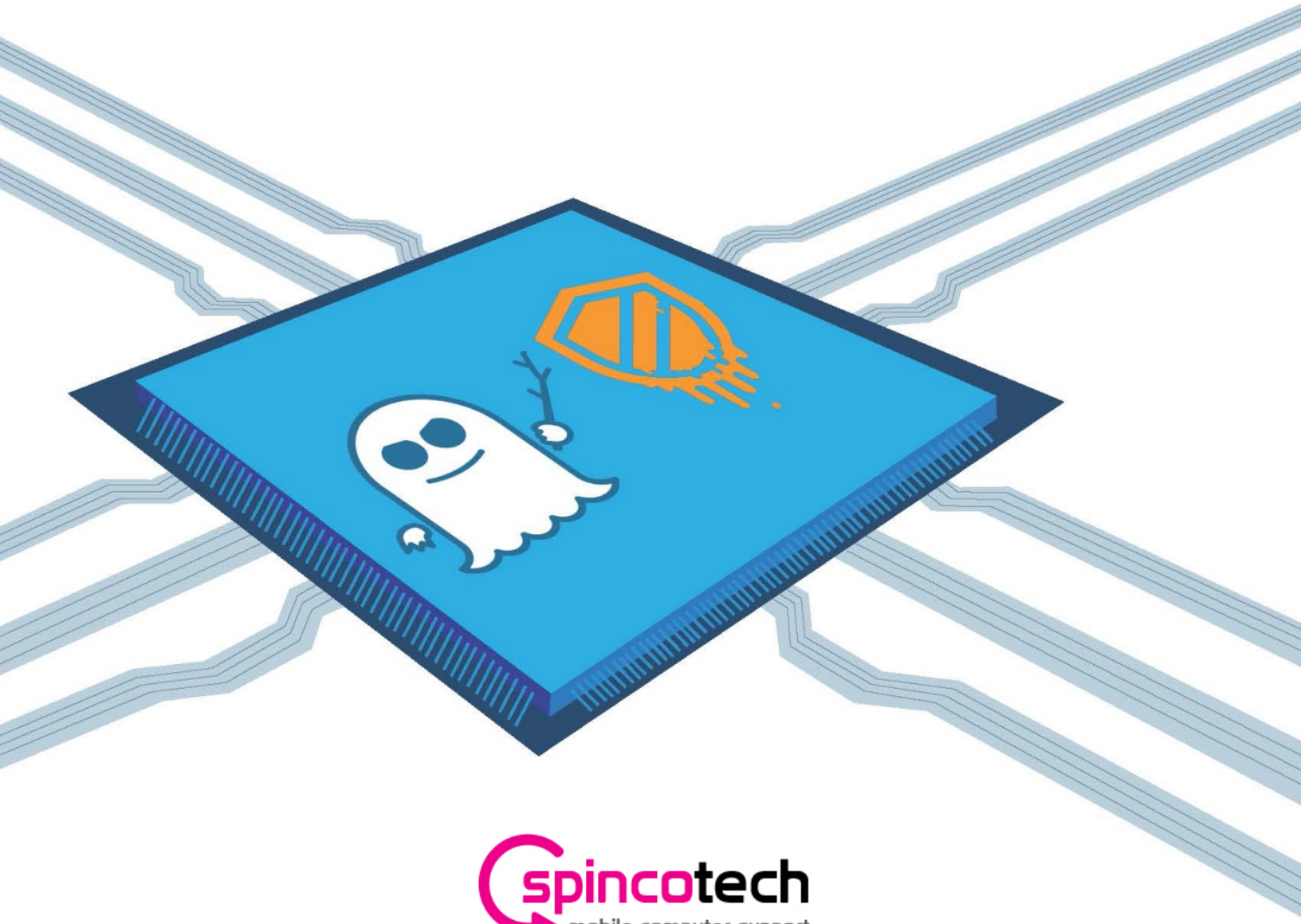
The CPU Flaw:

Spectre and Meltdown exposed

How you'll be affected



spincotech
mobile computer support

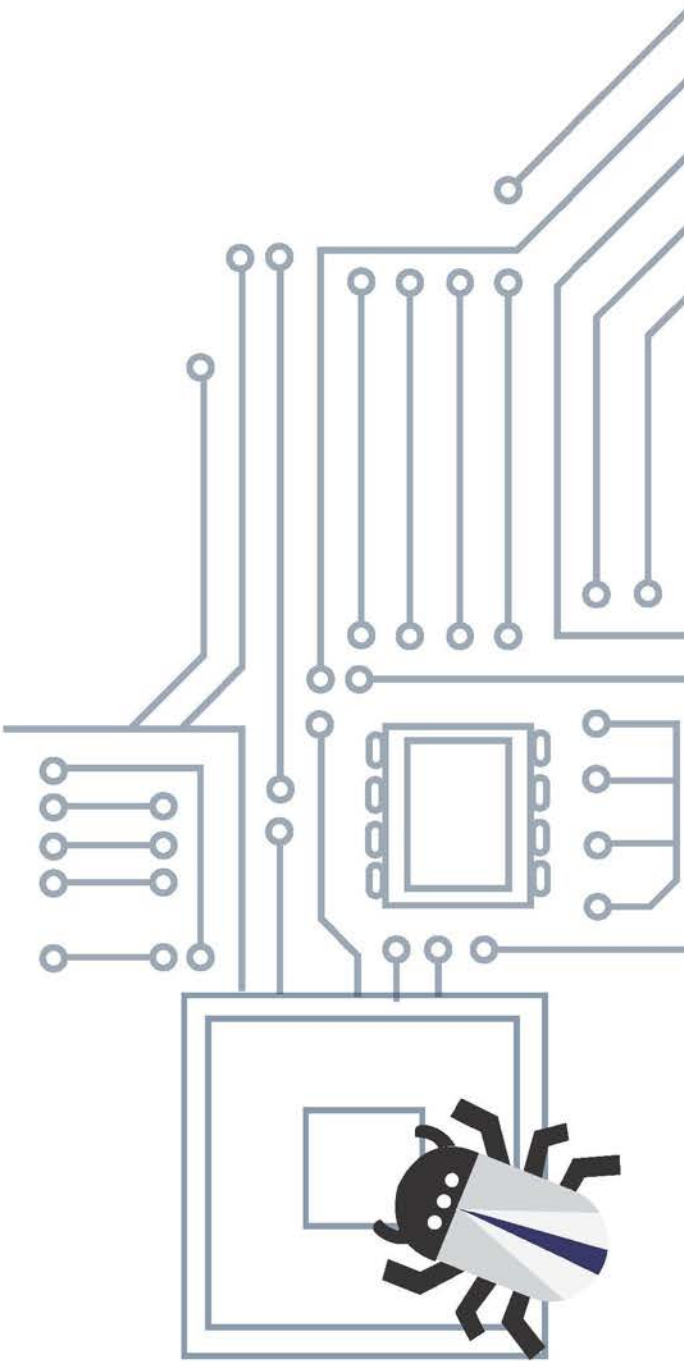
Summary

Severe design flaws in modern CPUs were recently discovered and made public. These flaws put users and businesses alike at risk of attacks known as *Spectre and Meltdown*, where private data can be called up and stolen. Chip manufacturers including Intel and ARM have responded by working with software developers to correct the flaws, however these fixes are affecting computer performance. Discover exactly how this vulnerability works, how you'll be impacted, and what you can do to protect your systems.

Spectre Meltdown
In a snapshot

What are Spectre and Meltdown?

In a bombshell report as we entered 2018, researchers revealed that nearly every computer chip is affected by a set of vulnerabilities called *Spectre and Meltdown.* The impact is so widespread because it's not a software issue from one developer, it's a flaw in the way computer chips were designed. All devices, including those made by Apple, Microsoft, Google, Amazon and others, share a similar chip structure. What's more, the flaws extend to servers, including Amazon Web Servers and Google Cloud.



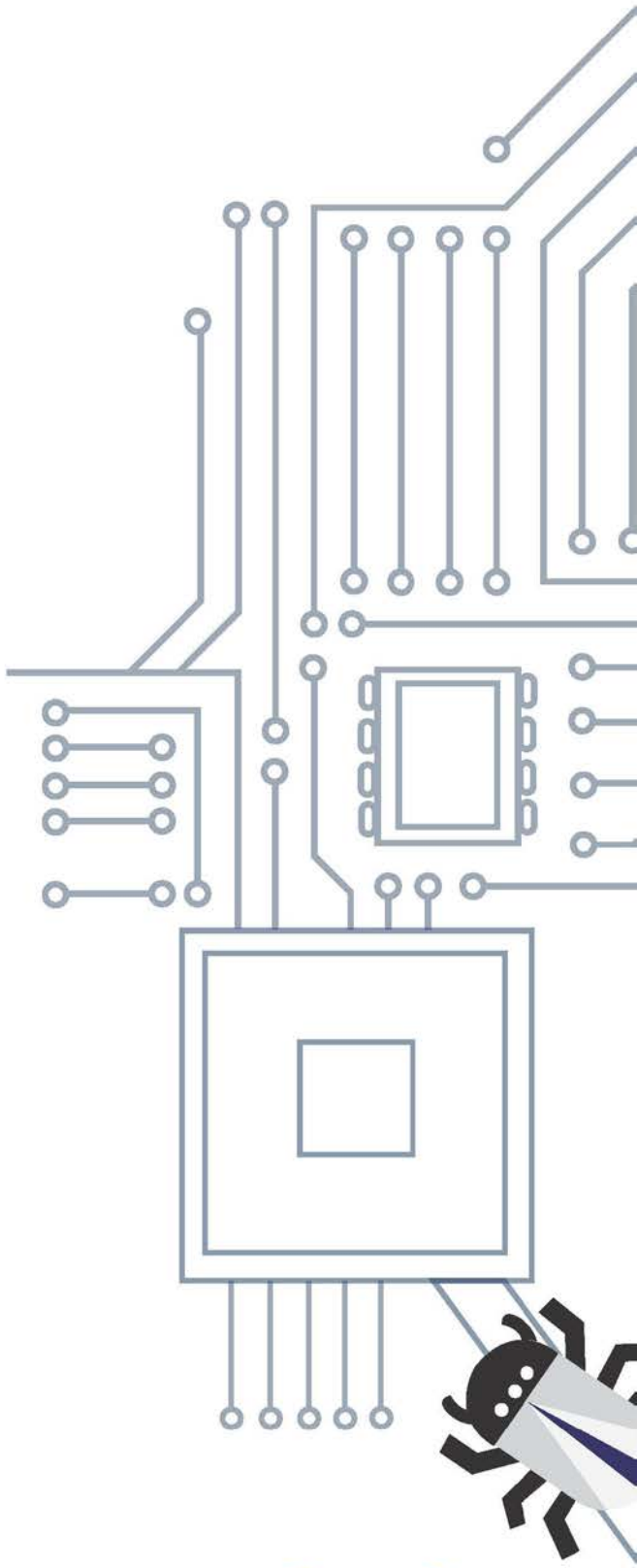
How They Work?

Your computer's CPU (its brain) does something called "speculative execution". It's part of the way processors were first designed, over 20 years ago. When your computer notices you do a task often, it tries to complete that task in the background, so it's ready before you need it. This speeds up your experience and makes your work easier.

Imagine strolling into your local coffee shop where they know your order is the same every day. Eventually, they anticipate that you'll be arriving at 8am sharp and have your coffee ready on the counter. However, if you change your mind and decide to order something else, they'll need to throw that coffee away.

Your CPU is doing the same thing. It's loading information like your credit card number or passwords, ready for you to do your usual tasks. If you change your routine and that information isn't needed, your CPU throws it away. Just like at the coffee shop though, the trash doesn't disappear immediately, so your credit card number and password are simply sitting there in a section of memory called the 'cache', waiting to be cleared away.

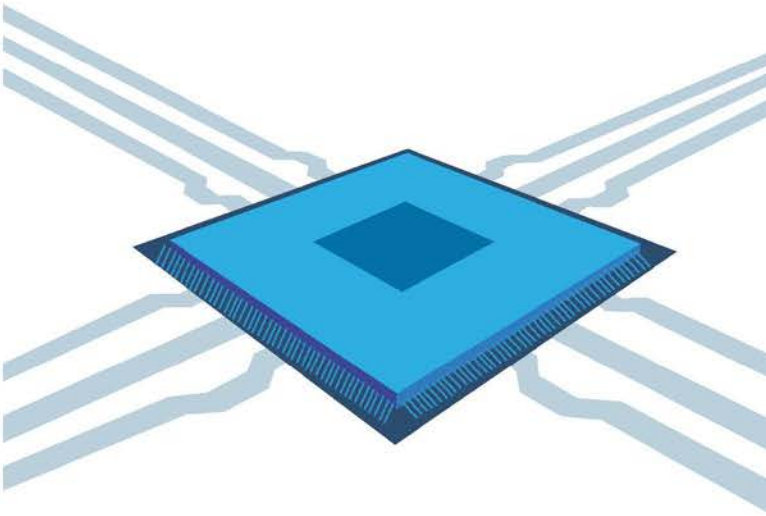
The Spectre vulnerability allows attackers to trick the processor into performing these speculative operations (loading up your private data), so that Meltdown can scoop it up from the trash.



How you'll be impacted

Developers are releasing emergency updates

Fortunately, this vulnerability isn't easy to exploit, and there have been no known attacks as yet. However, when the researchers went public with their discovery, it also alerted hackers to an opportunity. For them to get access to your system at this level though, they would first need to infect your computer with malware.



Most major companies such as Google, Apple and Microsoft were able to issue security updates before the flaw was announced. They're working closely with Intel, ARM and AMD, the main chip manufacturers, to mitigate the problem via software.

The current state of patches

- **Intel**

  According to Intel, they have "developed and rapidly issuing updates for all types of Intel-based computer systems — including personal computers and servers — that render those systems immune from both exploits."

- **Apple**

  An update for Safari is available and updates to iOS 11.2, macOS 10.13.2 and tvOS 11.2 have been released to defend against Meltdown. According to Apple statements, Apple Watch is not affected by either Meltdown or Spectre. Updates for older devices are not being released.

- **AMD**

  AMD initially advised their CPUs were not vulnerable at all, but have since acknowledged that Spectre is a potential threat to their systems and are working on a patch.

- **Microsoft**

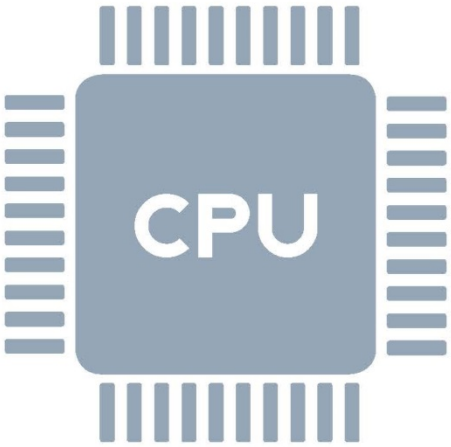
  Microsoft was quick to release updates for Windows 7, Windows 8.1, Windows 10 and various Windows Server versions. Updates for older versions are not being released and are working on a patch.

Patches for unaffected chips from Nvidia, IBM and AMD are also being rolled out to ensure these systems don't place others at risk.

Developers are releasing emergency updates

Windows 7 and 8 machines will be the most impacted
Windows 10 is safer from Spectre and Meltdown

Recall how the flaw exists due to speculative execution, a process designed to speed up your computing experience? The patches and updates have been changing the way your CPU uses memory, essentially putting the brakes on this shortcut. Developers were aware that slowdowns would occur but aimed to keep the impact to a minimum.



According to Terry Myerson, Microsoft VP, you can expect the following impact:

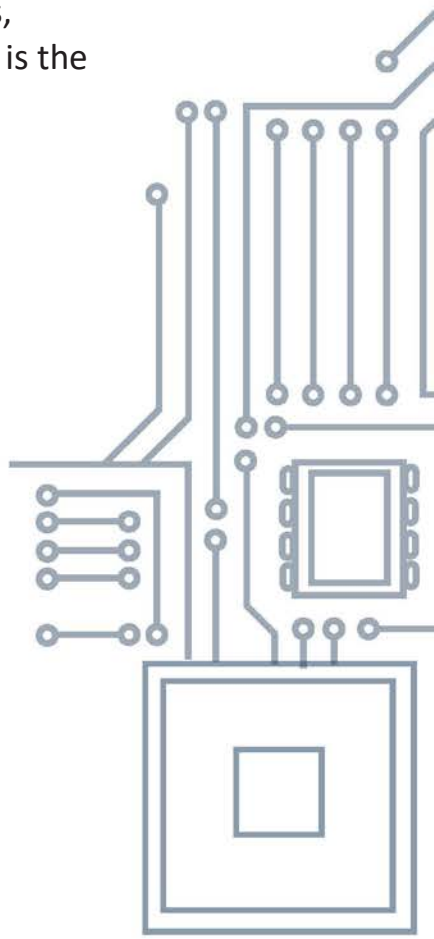
Windows 10 with newer CPU	Negligible
Windows 10 with older CPU	Noticeable decrease in performance
Windows 7, 8 with older CPU	Most noticeable decrease in performance
Windows Server (any CPU)	Significant impact

It's likely that further updates will be released to address these issues, however those with older CPUs or Operating Systems might find now is the time to upgrade.

How you can stay protected

Antivirus

As any attack will first need to come through malware such as viruses, be extra vigilant with your virus protection. Update your antivirus software regularly, and set your system to run full scans each week. Likewise, keep an eye out for phishing links that don't look quite right.



Run all updates

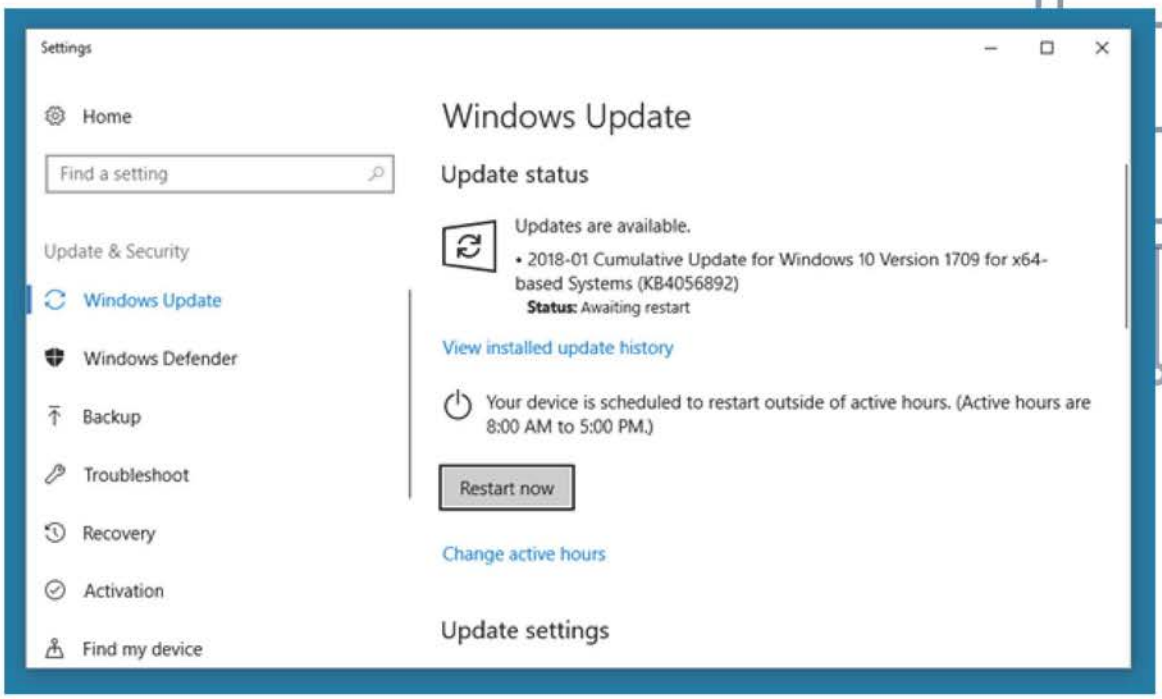
While nobody likes the idea of their computer slowing down, not even a fraction, it's better than having your credit card details or passwords stolen by a hacker. Be sure to run updates as soon as they are released.

Update firmware

Microsoft has advised that patches and updates aren't the complete fix to the Spectre and meltdown vulnerabilities, suggesting you also update your BIOS and firmware. As this can be a tricky process, we recommend that only trained technicians do this.

Upgrade your system

If your system is too old and didn't receive an emergency update, you'll need to upgrade. This might mean switching to a newer smartphone, faster CPU or supported operating system.



Where to now?

As dire as it all seems right now, this flaw has been around for over 20 years. The sky isn't falling and there's no reason to panic. Remember, there have no known instances of a Spectre/Meltdown attack yet, the tech world is simply closing ranks against hackers to ensure your risk is minimized. Developers and manufacturers are working together to help protect your system, and so are we. You're in good hands.

Our managed services can help keep you safe from Spectre/Meltdown. Call us today to discuss.

spincotech
mobile computer support

07 855 2169
www.spincotech.co.nz