Meltdown and Spectre FAQ: How the critical CPU flaws affect PCs and Macs

It varies widely depending on your hardware, operating system, and workload.

BY BRAD CHACOS and MICHAEL Simon

Massive security vulnerabilities in modern CPUs are forcing a redesign of the kernel software at the heart of all major operating systems. Since the issues—dubbed Meltdown and Spectre—exist in the CPU hardware itself, Windows, Linux, Android, macOS, iOS, Chromebooks, and other operating systems all need to protect against it. And worse, plugging the hole can negatively affect your PC’s performance.

Everyday home users shouldn’t panic too much though. Just apply all available updates and keep your antivirus software vigilant (go.pcworld.com/anti), as ever. If you want to dive right into the action without all...
the background information, we’ve also created a focused guide on how to protect your PC against Meltdown and Spectre (go.pcworld.com/pv5).

Here’s a high-level look at what you need to know about Meltdown and Spectre (go.pcworld.com/mell), in plain language. Be sure to read Google’s post on the CPU vulnerabilities if you like diving deep into technical details (go.pcworld.com/gopc).

**MELTDOWN AND SPECTRE CPU FLAW FAQ**

Editor’s note: This article was most recently updated to mention CPU patches causing reboots in Intel systems, and Gibson Research’s InSpectre CPU tool, which can tell you if your PC is protected against these flaws. Microsoft has also patched its patch for AMD systems, which had previously left them unable to boot.

**GIVE IT TO ME STRAIGHT—WHAT’S THE ISSUE HERE?**

Again, the CPU exploits in play here are extremely technical, but in a nutshell, the exploit allows access to your operating system’s sacrosanct kernel memory because of how the processors handle “speculative execution” (go.pcworld.com/spec), which modern chips perform to increase performance. An attacker can exploit these CPU vulnerabilities to expose extremely sensitive data in the protected kernel memory, including passwords, cryptographic keys, personal photos, emails, or any other data on your PC.

Meltdown is the more serious exploit, and the one that operating systems are rushing to fix. It “breaks the most fundamental isolation between user applications and the operating system,” according to Google. This flaw most strongly affects Intel processors because of the aggressive way they handle speculative execution, though a few ARM cores (go.pcworld.com/arm) are also susceptible.

Spectre affects AMD and ARM processors as well as Intel CPUs, which means mobile devices are also at risk. (We have a separate FAQ on how Spectre affects phones and tablets [go.pcworld.com/setq].) There may be no permanent hardware solution to Spectre, which “tricks other applications into accessing arbitrary locations in their memory.” Processor firmware updates can mitigate the
issue to some degree. Software also needs to be hardened to guard against it.

**WHAT'S A KERNEL?**
The kernel inside your operating system is basically an invisible process that facilitates the way apps and functions work on your computer, talking directly to the hardware. It has complete access to your operating system, with the highest possible level of permissions. Standard software has much more limited access. Here’s how The Register (go.pcworld.com/r514) puts it: “Think of the kernel as God sitting on a cloud, looking down on Earth. It’s there, and no normal being can see it, yet they can pray to it.”

**HOW DO I KNOW IF MY PC IS AT RISK?**
Short answer: It is. Yes, even if it’s a Mac (go.pcworld.com/s1t4).

Google says “effectively every” Intel processor released since 1995 is vulnerable to Meltdown, regardless of the OS you’re running or whether you have a desktop or laptop. (You can find a full list of affected Intel processors in this article [go.pcworld.com/1141] )

AMD processors aren’t affected by the Meltdown bug. But chips from Intel, AMD, and ARM are susceptible to Spectre attacks. AMD says (go.pcworld.com/amds) its hardware has “near zero” risk to one Spectre variant because of the way its chip architecture is designed, but AMD CPUs can still fall prey to another Spectre flaw.

Unsure if you’re already protected against Meltdown and Spectre? Gibson Research’s easy-peasy, free inSpectre tool (go.pcworld.com/1555) lets you know if you’ve already installed the necessary operating system and processor updates on your computer.

**HOW DO I STAY SAFE?**
Update all the things. The entire computer industry is moving as quickly as possible to patch in Meltdown and Spectre protections. Right now, you should update your operating
system, CPU firmware (if available), and web browser pronto. We’ve created a separate guide to staying safe from Meltdown and Spectre attacks (go.pcworld.com/atku) if you need more in-depth help.

Definitely make sure you’re running security software as well—advice that Intel also stresses. No known Meltdown and Spectre attacks have been seen in the wild, but that’s sure to change now that the details are public. Triggering the attacks requires hackers to have access to your PC. An antivirus suite keeps bad guys off your PC. And as always, only download software and apps from reputable sources to reduce the risk of malware infection.

WHAT PATCHES ARE ALREADY AVAILABLE?
Microsoft pushed out a Windows update protecting against Meltdown on January 3, the day that the CPU exploits hit headlines. Updates issued outside of Microsoft’s monthly “Patch Tuesdays” are rare, underlining the severity of this issue. Unfortunately, the emergency patch renders some AMD computers unbootable (go.pcworld.com/unboot)—mostly ones

with older Sempron and Athlon processors, judging by initial reports. Microsoft halted the roll-out of the patch on affected systems until the fix is fixed.

Intel is also publishing firmware updates for its processors. You’ll need to snag them from your PC, laptop, or motherboard maker (like HP or Gigabyte) rather than Intel itself. By January 12, Intel expects to have released firmware updates for 90 percent of processors released in the past five years to its partners, though it will take longer for PC makers to actually push those fixes out for their devices. Firmware updates for all CPUs released in the last five years should have rolled out by the end of January, at which point Intel “will then focus on issuing updates
for older products as prioritized by our customers,” CEO Brian Krzanich said (go.pcworld.com/brk).

Warning: The first round of Spectre CPU fixes can cause more frequent, unwanted system reboots in Intel CPUs released since 2011 (go.pcworld.com/unw). You still want to install them for safety, and Intel’s working to correct the issue.

AMD plans to release firmware updates (go.pcworld.com/amd) to protect against Spectre, with patches for Ryzen, Threadripper, and Epyc CPUs coming first, and older architectures later. They’re classified as optional, though, because AMD says its CPU architecture has “near zero” risk against the Spectre variant that requires a firmware update.

Apple quietly released against Meltdown in macOS High Sierra 10.13.2, which released on December 6, as well as in iOS and tvOS 11.2. Kernel patches are also available for Linux.

Chromebooks received protection in Chrome OS 63, which released on December 15. You can find a detailed list of how individual Chromebooks are affected here (go.pcworld.com/chvm). Furthermore, the Chrome web browser itself was updated to include an opt-in experimental feature called “site isolation” (go.pcworld.com/sisid) that can help guard against Spectre attacks.

Site isolation is trickier on mobile devices; Google warns that it can create “functionality and performance issues” in Android, and since Chrome on iOS is forced to use Apple’s WKWebView, Spectre protections on that platform need to come from Apple itself. Chrome 64 will include more mitigations.

Other browsers are batting down the hatches against Spectre as well. Firefox 57 (go.pcworld.com/657) came out in November with some initial safeguards, and Edge and Internet Explorer (go.pcworld.com/edie) received an update alongside Windows 10. On January 8, Apple pushed out updates to iOS 11 (go.pcworld.com/611) and macOS (go.pcworld.com/sf11) with “security improvements to Safari and WebKit to mitigate the effects of Spectre.”

Nvidia swiftly released graphics card drivers containing initial protection against Spectre (go.pcworld.com/rvd) as well—a crucial fix since GPU display drivers sink deep hooks into your kernel. Grab the latest Nvidia drivers here (go.pcworld.com/dr1).

Check out PCWorld’s guide to protecting your PC against Meltdown and Spectre (go.pcworld.com/me1) if you need more help.

Gibson Research’s dead simple (and free) InSpectre tool (go.pcworld.com/600) can let you know instantaneously if your PC has the necessary operating system and CPU patches installed.

**WILL THESE FIXES SLOW DOWN MY PC OR MAC?**

It’s complicated, and highly dependent on your hardware, operating system, and...
workloads.

More recent Intel processors from the Skylake (6th-gen Core i5/i7 series) era onward have a technology called PCD (Process Context Distinction) enabled and suffer less of a performance impact, according to Microsoft (go.pcworld.com_RESP0E). Your version of Windows makes a difference as well. Plus, some applications—most notably virtualization and data center/cloud workloads—are affected more than others. Intel confirmed that the performance loss will be dependent on workload, and “should not be significant” for average home computer users.

Windows chief Terry Myerson says they “don’t expect most users to notice a change” on Windows 10 systems running Intel 6th, 7th, or 8th-generation Intel processors.

Intel published some post-patch benchmark results (go.pcworld.com/m28) on best-case PCs like this one for its blog. The tests showed an average performance loss of between 2 and 7 percent in the SYSMark 2014 SE benchmark, which simulates productivity tasks and media creation. Its responsiveness score—which measures (go.pcworld.com/m28) “pain points” in the user experience when performing common activities—plummeted by a whopping 14 percent, though. In web applications that use heavy amounts of JavaScript, Intel saw a 7 to 10 percent performance loss post-patch. These tests were performed on SSD-equipped systems; Intel reports the performance loss is less noticeable if you’re using a traditional hard drive.

Those are the best-case scenarios, though.

If you’re running older processors, including 5th-gen Haswell chips, “some benchmarks show more significant slowdowns, and we expect that some users will notice a decrease in system performance,” Microsoft reports. Finally,
Intel's post-patch performance results on "best-case" PCs.

Microsoft says for PCs running one of those older Intel CPUs and the older Windows 7 or 8 operating systems, "we expect most users to notice a decrease in system performance." As far as business use cases, Windows Server "shows a more significant performance impact when you enable the mitigations to isolate untrusted code within a Windows Server instance."

Early consumer benchmarks conducted using the Windows patch alone showed the most performance impact in storage speeds, but Microsoft's Myerson stresses, "many of the benchmarks published so far do not include both OS and silicon updates," which he deems a crucial part of the performance puzzle. Intel's benchmarks include both OS and firmware updates.

"Obviously it depends on just exactly what you do," Linux creator Linus Torvalds wrote (go.pcworld.com/linus) in the Linux Kernel Mailing List. "Some loads will hardly be affected at all, if they just spend all their time in user space. And if you do a lot of small system calls, you might see double-digit slowdowns."
WILL MY GAMES GET SLOWER?

Nope, according to the limited testing performed so far, though these sources didn’t test the Meltdown and Spectre patches with updated CPU firmware.

Phoronix (go.pcworld.com/phor) tested Dota 2, Counter-Strike: Global Offensive, Deus Ex: Mankind Divided, Dawn of War II, F1 2017 and The Talos Principle on a Linux 4.15 rc6 machine with a Core i7-8700K and Radeon Vega 64 (go.pcworld.com/nv64). None saw a frame rate change outside the margin of error range.

Hardware Unboxed tested a handful of DirectX-based Windows games in the video linked above. With DirectX hooking so deeply into Windows, gamers were worried about a potential performance degradation there. Fortunately, Hardware Unboxed observed virtually no frame rate loss in Ashes of the Singularity, Assassin’s Creed: Origins, or Battlefield 1.

The Intel results cited in the previous section include both OS and firmware patches. It showed virtually no performance loss in 3DMark Sky Diver, a popular graphics benchmarking tool.

ARE AMD PROCESSORS AFFECTED?

Much, much less than Intel chips. All modern CPUs are vulnerable to Spectre attacks, but AMD says that its CPUs have “near zero” risk to the variant causing performance slowdowns in Windows PCs due to the way they’re constructed. Nevertheless, AMD is releasing CPU firmware updates to protect against it, though they’re classified as optional. Operating system and software updates will protect against the other Spectre variant.

There is “zero AMD vulnerability” to Meltdown thanks to chip design, AMD says. If operating system patches exclude AMD CPUs from the new Meltdown-related performance restrictions—and Linux definitely is—the performance war between Intel’s chips and AMD’s new Ryzen CPUs (go.pcworld.com/ryzn) may get even tighter.

The emergency Windows patch rendered some AMD PCs unbootable (go.pcworld.com/unbo), which prompted Microsoft to halt its installation on potentially impacted systems. It appears mostly older Sempron and Athlon CPUs are affected. Microsoft’s new patch, KB4073290, that solves the problem (go.pcworld.com/kb40), it will either deploy via Windows Update or can be manually downloaded (go.pcworld.com/m40).