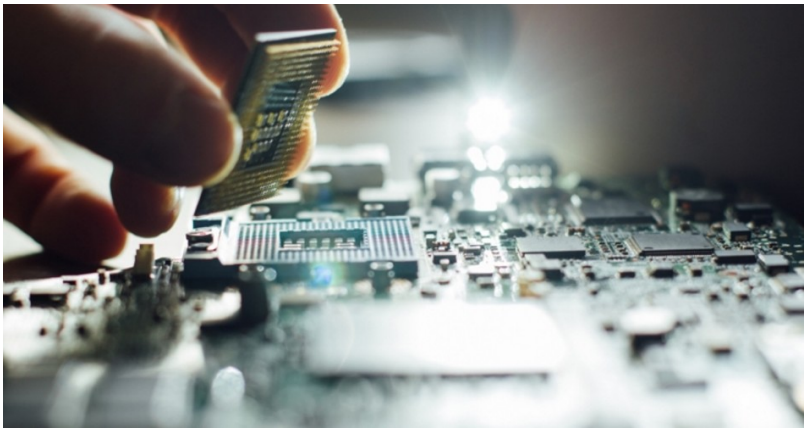
Written by **James Donlon** on January 10, 2018

Serious Hardware Flaw Cripples Most Basic Security for Millions of Devices



A newly discovered flaw in the central processing units (CPUs) of computers, mobile devices, and cloud computing devices puts users at risk of hacking — regardless of their software or operating system (OS). And the flaw affects virtually every computer, mobile device, and cloud computing device created in the last 20 years.

Just over a week ago, several security professionals, including Google's Project Zero, a few universities, and private security firms, found the flaw and two possible lines of attack that hackers can pursue based on this flaw. Project Zero named the attacks "Meltdown" and "Spectre." The hardware bug is part of Intel CPUs, and apparently was also found on AMD and ARM processors as well. The bug allows processes to delve into and access memory in the computer's kernel, the deepest and most privileged area of a machine. This spells disaster, as the exploit can spy on data and other processes, effectively escaping any type of security "sandbox." The worst part? It affects computers as well as smartphones and other devices, regardless of operating systems.

A very basic principle of software and computer security is "sandboxing" and application permissions. Basically, programs and code are isolated, or put in a virtual "sandbox" to play by themselves and only with the toys they are assigned. This prevents these programs from reaching into the proverbial cookie jar, because the cookie jar is hidden from them (for good reason). Isolation prevents applications from accessing things that would compromise security of the device, such as core OS components, root privileges, or even personal files and folders that have nothing to do with the application in question. This practice, which one can see on their mobile phone's "permissions," for example, is ubiquitous, thankfully. However, a serious flaw enables hackers to completely work around this security practice. The scary part is that while kernel developers are working on pushing out patches to fix the problem, those patches are slow in coming because the flaw is in the Core Processing Unit (CPU), the "brain" of literally millions of devices. The patches are a type of computer "brain surgery," and it takes time to do it correctly.

{modulepos inner_text_ad}

While the problem is pretty technical and somewhat difficult to explain to the average computer user, it

is serious enough that the entire industry is scrambling for a fix. Graz University of Technology in a joint effort has released a lengthy study — aptly named "Meltdown" — which says, in part, "On affected systems, Meltdown enables an adversary to read memory of other processes or virtual machines in the cloud without any permissions or privileges, affecting millions of customers and virtually every user of a personal computer." So while many people do not understand the problem itself, they are still put at risk by it. Literally anyone with the understanding and know-how to exploit Meltdown or Spectre (this certainly includes the folks over at the NSA and CIA) can access someone's computer or mobile device, regardless of the operating system installed on it. (Yes, that includes Linux too, believe it or not.)

As if this was not bad enough, apparently the flaw has been around for 20 years. While it was just discovered *publicly*, it is more than feasible that the flaw has been known by other, let's just say "less-public," entities. Just think about it. Would a person or agency that exploits vulnerabilities in order to surveil or monitor a target, or commit some other type of cyber-crime, want to alert the public, knowing that this wouild result in the exploit being patched? Of course not. So, pick the governmental spy agency or hacking group, the odds are hackers already knew about Meltdown and Spectre (and perhaps others) and are now vaguely humored as they read the headlines.

The good news is the entire tech community is well aware of this serious problem, and literally the best brains in the world are now working to fix the problem. While the majority who are not a part of the development community cannot actively do anything to fix the problem, good security practices are obviously still necessary. Early software patches and system updates are being developed and released across the board, which will mitigate the problem, hopefully very soon. The best practice for users is to apply whatever patches are issued as soon as they are available. Keeping your end-point devices up-to-date is always a good idea.

Photo: golubovy/iStock/Getty Images Plus