The CYBER GURU

Ed Kipp
Cybersecurity

Meltdown is an exploit that affects all Intel microprocessors built since 1995, with very limited exceptions. The processor is essentially the brain of any device, and Meltdown is like a genetic defect, something in the makeup of the processor that is vulnerable to certain attacks or conditions. It would be like a child being born with torn knee cartilage; Meltdown is similar in that there is an inherent vulnerability during the manufacturing process.

There are patches available for Meltdown, but they are akin to putting a knee brace on – it will help with stability but it sacrifices performance (studies show anywhere between 5 and 30 percent). Moreover, the patches are for the operating systems (Windows, MAC OS, Linux, IOS, Android, and IoT), so they just remove access to the flaw within the processor. A true fix for the processor would require a firmware update, and with the sheer number of processors affected, that seems unlikely.

There have been no reported hacking attempts using the Meltdown vulnerability, but the need for patching has caused problems. There have been some driver incompatibilities, conflicts with security software, and even bogus patches containing malware. Some people are choosing to ignore the patches in order to maintain performance and are therefore choosing convenience over security. Their thought process is simple – while it is possible that a smart IoT device like a thermostat could be compromised, if it doesn't have the ability to download and run new code, its usability when compromised is not worth the time for the bad actor. However, if they are in charge of servers containing important data, choosing performance over security would be a mistake.