Issued 1/7/18

How Big Tech Has Left You in the Dark about Massive CPU Flaws

The of deep-seated processor vulnerabilities going by the names “Meltdown” and “Spectre,” may be the biggest news in computing security in years, but you wouldn’t know that from the sites of some of the companies that should be your first line of defense. These firms have known about these vulnerabilities longer than most–researchers told them last summer, after first detecting the issue. Having the public disclosure planned for next week moved up after word began to leak should not have left non-techie users with so much to puzzle through when looking for help from the firms behind your devices.

Meltdown and Spectre’s two variations take advantage of how modern processors try to work faster by skipping ahead of themselves. They predict the operations that will come up next, then run those tasks sooner. Teams of researchers found that by timing this back-and-forth of data, a rogue app could start to see system-level data— for example, saved passwords — that would normally be off limits. Having hostile code running on your computer is already a problem you would have had to solve, but this escalates its potential damage. Meltdown, which appears confined to the Intel processors that run most PCs and all Macs, is easier to exploit but easier to patch. Spectre also afflicts AMD processors as well as the ARM chips in many mobile devices.

Google, developer of the Chrome browser and the Android mobile operating system, offers the most information. A post on its primary blog [link] points readers to a more technical note that, in turn, points to a detailed how-to that explains that the latest Android security update and a Chrome option separately address these vulnerabilities. (To enable that “site isolation” option, which may cause Chrome to eat more memory, type “chrome://flags#enable-site-per-process” into its address bar, then click the “Enable” button that appears.) A Microsoft tech-support note reports that patches are on the way via the company’s Windows Update system. Microsoft also says that third-party antivirus apps may also block an exploit from being installed. The post also reminds users that they’ll need firmware updates from their computer vendors.

A far-less-obvious post on a Microsoft developer blog documents another option for impatient users or those with uncooperative third-party security tools: visit Microsoft’s Update Catalog site, search for “KB4056890” and pick the right download for your processor architecture. Apple has yet to talk about this on its customer site, its developer site or its @AppleSupport Twitter account.