Meltdown microprocessors

Specter and MELTDOWN Researchers have recently discovered a design flaw that results in a security vulnerability in the CPU chip that powers the majority of all the world’s computers, including PCs, mobile devices, and servers. This CPU bug allows malicious programs to view data that is being processed in the computer memory. Meltdown is a vulnerability affecting Intel x86 microprocessors and some ARM-based microprocessors. Unlike the related Meltdown vulnerability disclosed at the same time, Spectre does not rely on a specific feature of a single processor's memory management and protection system but is a more generalized vulnerability. The first reports were published on January 2, 2018, prior to a coordinated disclosure scheduled for the week of January 8. There is no evidence of exploitation at this time, but the publicly disclosed proof-of-concept (PoC) exploit code could result in the vulnerabilities being weaponized for malware delivery.

Further Details

Specter and MELTDOWN are what is known as `speculative execution side-channel attacks.` These attacks exploit performance optimizations used by modern CPUs to access protected memory. Basically, the main chip in most modern computers—the CPU—has a hardware bug. This design flaw has been present since the 1990’s. Normally, applications and the operating system are isolated from each other, so data is not accessible. This hardware flaw breaks that isolation. This means there is a primary risk of malicious actors being able to get access to the encryption keys or your passwords stored in a password manager or browser, your emails, instant messages, donor information, and the like. Cloud servers could be significantly impacted if an attacker exploits these vulnerabilities to break out of a guest virtual host or container. It may also be possible to deliver exploit code via drive-by download to extract information from a victim’s web browser. At this time, limited practical demonstrations of these attack vectors exist. These vulnerabilities have been assigned the following CVEs: - CVE-2017-5753: Bounds check bypass (SPECTRE) - CVE-2017-5715: Branch target injection (SPECTRE) - CVE-2017-5754: Rogue data cache load (MELTDOWN) Intel, AMD, ARM, Microsoft, Google, Apple, Amazon, and other technology vendors are releasing software updates to mitigate the risk from these vulnerabilities. Long-term solutions require re-engineering the vulnerable processor architectures.

A third-party analysis of vendor security updates notes potential performance impact under some circumstances and workloads, as well as conflicts between the OS patches and some software that has significant interactions with the kernel (e.g., antivirus and endpoint security solutions). What should you do about this? Updates and patches are needed for all computers,

servers, and other equipment with a CPU. There will most likely be patches for your antivirus software, your operating system software, workstation software, and firmware patches to physical machines themselves. The full patch analysis and patch cycle may take some time because some of the vulnerable component patches are not yet available. Microsoft Azure and Amazon AWS are already in the process or have already patched customer systems hosted on those respective platforms. CTU researchers strongly advise a phased approach to updating vulnerable systems. Once the patches are available, organizations should follow standard best practices for testing updates on systems that match the production environment and should test a subset of updated systems with a representative workload before widely deploying updates in production environments. Databases or systems with high levels of I/O activity may be most significantly impacted.

Organizations should also contact cloud service providers to confirm that platforms that store or process corporate data are updated, especially for shared hosting or infrastructure-as-a-service providers" In the meantime, we recommend that organizations be extra vigilant, and communicate awareness of these vulnerabilities across your organization so that security stays at the top of mind."