About speculative execution vulnerabilities in ARM-based and Intel CPUs

Security researchers have recently uncovered security issues known by two names, Meltdown and Spectre. These issues apply to all modern processors and affect nearly all computing devices and operating systems. All Mac systems and iOS devices are affected, but there are no known exploits impacting customers at this time. Since exploiting many of these issues requires a malicious app to be loaded on your Mac or iOS device, we recommend downloading software only from trusted sources such as the App Store. Apple has already released mitigations in iOS 11.2, macOS 10.13.2, and tvOS 11.2 to help defend against Meltdown. Apple Watch is not affected by either Meltdown or Spectre. In the coming days we plan to release mitigations in Safari to help defend against Spectre. We continue to develop and test further mitigations for these issues and will release them in upcoming updates of iOS, macOS, and tvOS.

Background

The Meltdown and Spectre issues take advantage of a modern CPU performance feature called speculative execution. Speculative execution improves speed by operating on multiple instructions at once—possibly in a different order than when they entered the CPU. To increase performance, the CPU predicts which path of a branch is most likely to be taken, and will speculatively continue execution down that path even before the branch is completed. If the prediction was wrong, this speculative execution is rolled back in a way that is intended to be invisible to software.

The Meltdown and Spectre exploitation techniques abuse speculative execution to access privileged memory—including that of the kernel—from a less-privileged user process such as a malicious app running on a device.

Meltdown

Meltdown is a name given to an exploitation technique known as CVE-2017-5754 or "rogue data cache load." The Meltdown technique can enable a user process to read kernel memory. Our analysis suggests that it has the most potential to be exploited. Apple released mitigations for Meltdown in iOS 11.2, macOS 10.13.2, and tvOS 11.2. watchOS did not require mitigation. Our testing with public benchmarks has shown that the changes in the December 2017 updates resulted in no measurable reduction in the performance of macOS and iOS as measured by the GeekBench 4 benchmark, or in common Web browsing benchmarks such as Speedometer, JetStream, and ARES-6.

Spectre

Spectre is a name covering two different exploitation techniques known as CVE-2017-5753 or "bounds check bypass," and CVE-2017-5715 or "branch target injection." These techniques potentially make items in kernel memory available to user processes by taking advantage of a delay in the time it may take the CPU to check the validity of a memory access call.

Analysis of these techniques revealed that while they are extremely difficult to exploit, even by an app running locally on a Mac or iOS device, they can be potentially exploited in JavaScript running in a web browser. Apple will release an update for Safari on macOS and iOS in the coming days to mitigate these exploit techniques. Our current testing indicates that the upcoming Safari mitigations will have no measurable impact on the Speedometer and ARES-6 tests and an impact of less than 2.5% on the JetStream benchmark. We continue to develop and test further mitigations within the operating system for the Spectre techniques, and will release them in upcoming updates of iOS, macOS, and tvOS. watchOS is unaffected by Spectre.