Rajon, Md.Tarek Mahmud

id: 14-26557-2

Meltdown and Spectre :

Meltdown and Spectre are closely related vulnerabilities that can be exploited to abuse this process in different ways, allowing malicious programs to get access to data they shouldn't have. Meltdown read the contents of private kernel memory from an unprivileged user process.All out-of-order Intel processors released since 1995 with the exception of Itanium and pre-2013 Atoms. A list of vulnerable ARM processors and mitigations is listed here. No AMD processors are affected by Meltdown.

Spectre extract information from other running processes.Intel, ARM, and AMD processors are all reportedly affected to some degree.Apple has issued Spectre mitigations in iOS 11.2.2, and the macOS High Sierra 10.13.2 supplemental update.Meltdown allows kernel memory read.On the other hand spectre don't allow kernel memory read.Meltdown was patched with KAISER/KPTI.Meltdown leaks arbitrary user memory.Spectre also do that.Sometimes Meltdown could be executed remotely.But spectre definitely could be executed remotely.Meltdown do the practical attacks against Intel.Spectre do the practical attacks against Intel,AMD,ARM.