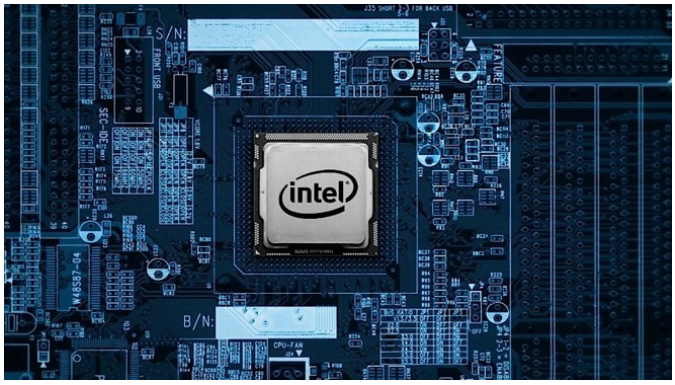
Researchers at the Worceseter Polytechnic Institute, Masschusetts, USA and the University of Lübeck, Germany warn of a new speculative execution security flaw present in modern Intel Core processors.



Dubbed "SPOILER" (or "Speculative Load Hazards Boost Rowhammer and Cache Attacks"), the flaw potentially allows attackers to extract passwords, keys and other data from memory using malicious JavaScript in a web browser. As such it is reminiscent of the Spectre vulnerabilities discovered earlier last year, although the researchers say the SPOILER flaw comes from a different hardware unit, the Memory Order Buffer.

For the curious, speculative execution involves using a memory order buffer to track operations by copying data from a CPU register to main memory, in the order it appears in code. As a result, data can be copied from the main memory to a register out of order, potentially speeding up the overall speed of operation if the speculative elements are right. If wrong, the speculative elements are discarded and a normal non-speculative data load is performed, meaning the instruction is carried out without the potential performance boost.

The researchers point out an issue with the Intel performance of memory disambiguation. The vulnerability is a question of timing, and the researchers managed to take advantage of it through an algorithm able to provide clues about memory locations. The team says the technique can make existing cache and "Rowhammer" attacks easier to perform, while enabling attacks using JavaScript to take seconds, not weeks, to complete.

Intel was notified of the vulnerability on December 2018, and disclosed to the public following the typical 90-day grace period. Intel is still to issue a CVE number for SPOILER, which is understandable due to it being not easily patchable with microcode. That said, the issue affects

all Intel Core processors, from the 1st generation down to the latest, regardless of OS.

In turn, Chipzilla states "we expect that software can be protected against such issues by employing side channel safe development practices. This includes avoiding control flows that are dependent on the data of interest. We likewise expect that DRAM modules mitigated against Rowhammer style attacks remain protected."

Go SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks