ZDNet

All Intel chips open to new Spoiler non-Spectre attack: Don't expect a quick fix...

Researchers say Intel won't be able to use a software mitigation to fully address the problem Spoiler exploits.

All Intel chips open to new Spoiler non-Spectre attack: Don’t expect a quick fix

Researchers say Intel won’t be able to use a software mitigation to fully address the problem Spoiler exploits.

Researchers have discovered a new flaw affecting all Intel chips due to the way they carry out speculative execution for CPU performance gains.

Like the Spectre and Meltdown attacks revealed in January 2018, Spoiler also abuses speculative execution in Intel chips to leak secrets.

However, it targets a different area of the processor called the Memory Order Buffer, which is used to manage memory operations and is tightly coupled with the cache.

Researchers from Worcester Polytechnic Institute, Massachusetts, and the University of Lübeck in north Germany detail the attack in a new paper, ‘Spoiler: Speculative load hazards boost Rowhammer and cache attacks’. The paper was released this month and spotted by The Register.

The researchers explain that Spoiler is not a Spectre attack, so it is not affected by Intel’s mitigations for it, which otherwise can prevent other Spectre-like attacks such as SplitSpectre.

“The root cause for Spoiler is a weakness in the address speculation of Intel’s proprietary implementation of the memory subsystem, which directly leaks timing behavior due to physical address conflicts. Existing Spectre mitigations would therefore not interfere with Spoiler,” they write.

They also looked for the same weakness in Arm and AMD processor cores but didn’t find the same behavior that is present in Intel chips.

Spoiler depends on “a novel microarchitectural leakage, which reveals critical information about physical page mappings to user space processes”.

“The leakage can be exploited by a limited set of instructions, which is visible in all Intel generations starting from the 1st generation of Intel Core processors, independent of the OS, and also works from within virtual machines and sandboxed environments.”

The researchers say that Spoiler improves Rowhammer attacks and cache attacks that reverse-engineer virtual-to-physical address mapping. Using Spoiler, they show the leakage can be used to speed up reverse-engineering by a factor of 256. It also can speed up JavaScript attacks in the browser.

The researchers say that Intel has confirmed receipt of their findings on December 1, 2018. However, they note Intel won’t be able to use a software mitigation to fully address the problem Spoiler exploits. Meanwhile hardware mitigations could address the issue but would almost certainly mean a hit on CPU performance.

They note that for JavaScript-based Spoiler attacks via a website, browsers could mitigate Spoiler by removing accurate timers, but removing all timers could be impractical.

Daniel (Ahmad) Moghimi, one of the paper’s authors, told The Register he doubts Intel will be able to patch the issue in the memory subsystem within the next five years.

“My personal opinion is that when it comes to the memory subsystem, it’s very hard to make any changes and it’s not something you can patch easily with a microcode without losing tremendous performance,” he said.

“So I don’t think we will see a patch for this type of attack in the next five years and that could be a reason why they haven’t issued a CVE.”

An Intel spokesperson said in a statement that software can be protected from Spoiler attacks while DRAM modules with Rowhammer mitigations still should remain shielded.

“Intel received notice of this research, and we expect that software can be protected against such issues by employing side channel safe software 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. Protecting our customers and their data continues to be a critical priority for us and we appreciate the efforts of the security community for their ongoing research.”