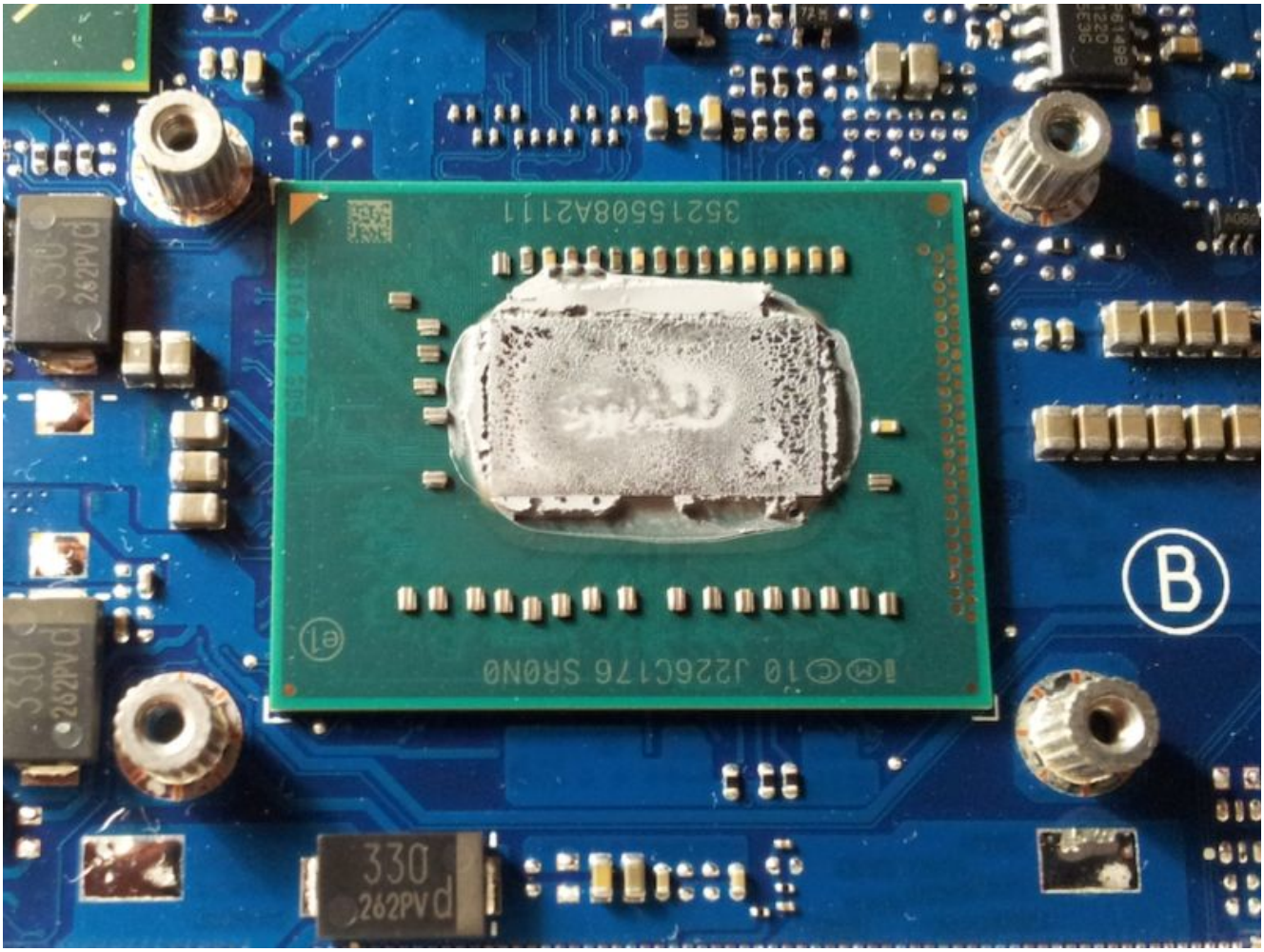
Silent Windows update patched side channel that leaked data from Intel CPUs



Enlarge / An uncovered Intel Core i5-3210M (BGA) inside of a laptop.

reader comments

43 with 34 posters participating, including story author

Share this story

Microsoft last month pushed a silent update that mitigated a serious vulnerability in all CPUs Intel has introduced since 2012, researchers who discovered the flaw said Tuesday.

The vulnerability—discovered and privately reported to Intel 12 months ago—resided in every CPU Intel has introduced since at least its Ivy Bridge line of processors and possibly earlier, a researcher from security firm Bitdefender told Ars. By abusing a performance capability known as speculative execution, attackers could open a side channel that leaks encryption keys, passwords, private conversations, and other secrets that are normally off limits.

The attack demonstrated in a research paper published by Bitdefender is similar to those disclosed in January 2018 under the names Spectre and Meltdown. Patches Microsoft released around the same time largely blunted those attacks. Microsoft's advisory described the flaw occurring "when certain central processing units (CPU) speculatively access memory," without mentioning Intel or any other chip maker. Bitdefender researchers, meanwhile, said they tested two AMD chips and found no evidence either was affected.

Bitdefender's researchers found that a chip instruction known as SWAPGS made it possible to revive the side channel, even on systems that had the earlier mitigations installed. SWAPGS gets called when a computing event switches from a less-trusted userland function to a more sensitive kernel one. Proof-of-concept exploits developed by Bitdefender invoked the instruction to siphon contents normally restricted to kernel memory into user memory.

"What we have found is a way to exploit the SWAPGS instruction which switches from userland to kernel mode in such a way that we could… carry out a side-channel attack," Bogdan Botezatu, Bitdefender's director of threat research and reporting, told Ars. "By doing that, we are going to leak kernel memory into the user space even if there are security measures that should prevent us from doing that."

Speculative execution attempts to make computers run faster by predicting instructions before they're actually given by an

application or operating system. When a predicted instruction doesn't actually come to be, it's supposed to be discarded as if it had no effect. The Spectre and Meltdown research, however, showed that the effects can still be found in the lowest-level architectural features of the processor.

Speculatively executed instructions can load data into cache even though the instruction is later aborted. That data can then be detected and inferred by other processes, since accessing it will be slightly faster than if it wasn't cached. Other data in the processor, including predictions about which instruction branch should be followed, can similarly be probed for clues about sensitive information.

The vulnerability found by Bitdefender affects all Intel CPUs that support SWAPGS and another instruction called WSGRBASE. Bitdefender researchers said, at a minimum, this includes all processor lines since Ivy Bridge. But Botezatu said it's possible earlier chips are also affected. Bitdefender was able to exploit the side channel when chips ran Windows. Botezatu said that, while the vulnerability technically exists when affected chips run on other operating systems, it was "unfeasible" to exploit chips running Linux, Unix, FreeBSD, or macOS.

Exploiting the vulnerability using JavaScript is not possible, so that makes website drive-by attacks unfeasible as well.

Microsoft silently patched the vulnerability during last month's update Tuesday. Microsoft said the fix works by changing how the CPU speculatively accesses memory. The fix doesn't require a microcode update from computer manufacturers. The vulnerability is tracked as CVE-2019-1125.

A Microsoft representative wrote in a statement:

> *We're aware of this industry-wide issue and have been working closely with affected chip manufacturers and industry partners to develop and test mitigations to protect our*

> *customers. We released security updates in July, and customers who have Windows Update enabled and applied the security updates are protected automatically.*

An Intel representative wrote: “Intel, along with industry partners, determined the issue was better addressed at the software level and connected the researchers to Microsoft. It takes the ecosystem working together to collectively keep products and data more secure, and this issue is being coordinated by Microsoft.”

Red Hat said in a statement that the vulnerability affected both Intel and AMD chips and urged users to update systems “as soon as errata are available.” Bitdefender researchers, for their part, said they tested two AMD processors and “neither exhibited speculative behavior for the SWAPGS instruction.” In a statement, AMD officials wrote:

> *AMD is aware of new research claiming new speculative execution attacks that may allow access to privileged kernel data. Based on external and internal analysis, AMD believes it is not vulnerable to the SWAPGS variant attacks because AMD products are designed not to speculate on the new GS value following a speculative SWAPGS. For the attack that is not a SWAPGS variant, the mitigation is to implement our existing recommendations for Spectre variant 1.*

Bitdefender researchers described two attack scenarios. The first is when SWAPGS isn’t being executed speculatively when it should, and the second is just the opposite, when SWAPGS is being executed speculatively and should not be.

Each scenario had two variants: (1) when the attacker detects a value located at a specific kernel address and (2) when the attacker finds a value at a random kernel address. AMD’s statement indicates that its processors are affected only by the second variant of the second scenario. The statement also

indicates that existing Spectre mitigations are effective in this case.

The most likely scenario for exploitation would be against a cloud service, most likely by hackers working for a nation-state. The vulnerability makes it possible for one virtual machine to steal secrets residing inside of another virtual machine running on the same vulnerable CPU.

The exploit would “make sense for a state-sponsored attacker that has access to resources in a multi-tenant environment,” Botezatu said. Even in that scenario, it would take hours for secrets to leak out. Still, he said, running the exploit over periods as long as a year might be possible, since there’s no easy way to detect it.

The Bitdefender paper said researchers first reported the vulnerability to Intel 12 months ago, on August 7, 2018. Intel responded three weeks later by saying it already knew of the vulnerability and had no plans to fix it. Bitdefender said it spent the next eight months insisting to Intel that the behavior was problematic. Intel finally confirmed the leak of kernel memory on April 2 and indicated that a fix would come from fixes in operating systems.

Microsoft confirmed to Bitdefender it was investigating the leak on April 17. Bitdefender provided a new proof-of-concept exploit on April 22. On May 7, Microsoft reported it was able to reproduce the leak and would attempt to release a patch in July.

While the vulnerability isn’t likely to be widely exploited—if at all—it’s a testament to the difficulty of completely patching a new class of CPU flaws that stem from speculative execution. Since Spectre was disclosed 19 months ago, researchers have unearthed a raft of related ones. Don’t be surprised if more follow in the coming months or years.

https://arstechnica.com/?p=1547147