Microsoft patch eases jitters over SWAPGS vulnerability

August 8 2019, by Nancy Cohen

Credit: CC0 Public Domain

Plain and simple, it began as worrying security news. Bitdefender researchers identified and demonstrated a new side-channel attack. The flaw could allow attackers to access sensitive data stored in the kernel,

said Phil Muncaster, *Infosecurity Magazine*, on Aug. 7, Wednesday.

News had been made at the Black Hat security conference. Bitdefender provided a proof-of-concept attack that showed how the vulnerability could be exploited. Bitdefender disclosed the flaw in conjunction with Microsoft.

An alarm was sounded that a vulnerability was affecting modern Intel processors and could place both consumers and enterprises at risk.

Bitdefender said, "we demonstrate a new type of side-channel attack based on speculative execution of instructions inside the OS kernel. This attack is capable of circumventing all existing protective measures, such as CPU microcode patches or kernel address space isolation (KVA shadowing/KPTI)."

This attack takes advantage of a combination of Intel speculative execution of a specific instruction (SWAPGS) and use of that instruction by Windows operating systems within what is known as a gadget, said Bitdefender. The SWAPGS Attack affects newer Intel CPUs that use speculative execution, it said.

Bitdefender can explain what is behind the vulnerability: "In pursuit of ever-faster CPUs, vendors have implemented various versions of speculative execution. This functionality has the CPU making educated guesses about instructions that may be required before it determines whether the instructions are, in fact, required. This speculative execution may leave traces in cache that attackers can use to leak privileged, kernel memory."

Forbes, on August 6, carried a quote from Bogdan Botezatu, director of threat research and reporting at Bitdefender: "We call this the SWAPGS attack because the vulnerability leverages the SWAPGS instruction, an

under-documented instruction that makes the switch between user-owned memory and kernel memory."

Paul Wagenseil, *Tom's Guide*, described SWAPGS as "a kernel-level instruction set introduced with Intel's Ivy Bridge processors in 2012 that can be speculatively executed in user mode."

The following was the AMD statement.

"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."

Tom's Guide on Linux: "The flaw is less serious on Linux machines running Intel chips, and Bitdefender were not able to provide a proof-of-concept exploit for Linux."

As for Microsoft? By August 6 the bad news was at least good in terms of response. A "Silent Windows update" had patched the side channel leaking data from Intel CPUs, said *Ars Technica.*

Microsoft emerged as a key player in bringing about a fix. Reports pointed to Microsoft last month secretly fixing a security flaw in Intel chips "that could have reversed all the fixes made by either company in the wake of the Spectre and Meltdown vulnerabilities," said Wagenseil in *Tom's Guide*.

Dan Goodin in *Ars Technica* reported that "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."

Intel, in a statement provided to *The Register*, said, "Intel, along with industry partners, determined the issue was better addressed at the software level and connected the researchers to Microsoft," the chipmaker said. "It takes the ecosystem working together to collectively keep products and data more secure and this issue is being coordinated by Microsoft."

Spectre is a flaw that if exploited could force a program to reveal data. The name derives from "speculative execution"—an optimization method a computer system performs to check whether it will work to prevent a delay when actually executed. Spectre affects devices including desktops, laptops and cloud servers.

Bitdefender said that they expected that Apple devices were NOT vulnerable, "but we must wait for their official position once everything is released."

Here is the statement from Microsoft: "On August 6, 2019 Intel released details about a Windows kernel information disclosure vulnerability. This vulnerability is a variant of the Spectre Variant 1 speculative execution side channel vulnerability and has been assigned CVE-2019-1125. On July 9, 2019 we released security updates for the Windows operating system to help mitigate this issue. Please note that we held back documenting this mitigation publicly until the coordinated industry disclosure on Tuesday, August 6, 2019. Customers who have Windows Update enabled and have applied the security updates released on July 9, 2019 are protected automatically. There is no further configuration necessary."

Red Hat issued a statement too, "CVE-2019-1125: Spectre SWAPGS gadget vulnerability."

All in all, said Bleeping*Computer*, "In a coordinated disclosure, numerous vendors including Microsoft, Red Hat, Intel, and Google have released advisories regarding this vulnerability."

So, a troubling vulnerability and an impressive response. What do we learn from all the noise? Dan Goodin had an answer. "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."