Intel casts third patch to battle MDS Goliath

30 January 2020, by Nancy Cohen

Credit: CC0 Public Domain

What does a chip giant gotta do? ZombieLoad won't die and that is not to be allowed. Intel has forced out a third patch, said reports.

Joel Hruska in ExtremeTech on Wednesday wrote that "Intel has released a patch for the Zombieload / MDS (microarchitectural data sampling) security flaws that it first announced last year. This is the third set of patches related to those flaws, though only one of the two fixes even rates 'Medium' severity."

Patch patch patch. What happened to the first two? In May last year, said Darren Allan, *TechRadar*, Intel released the first patch. The second patch came in November, "to prevent a further type of attack not covered with that first fix." He wrote that Intel issued "another—third—patch to fix a couple of new variations on the ZombieLoad security flaw which poses a threat to the chip giant's processors."

How much of a headache?

"ZombieLoad is still very much a living nightmare for Intel," said Allan, "particularly following other high-profile speculation execution vulnerabilities which have affected the company's chips in the past, such as Meltdown and Spectre."

As for people trying to read about the vulnerabilities found by researchers, it is possible that you could find it complicated, between name tags, variants and patch details.

Fortunately, Andy Greenberg in Wired gave readers an overview of what has taken place and how Intel responded.

"Over the last two years, security researchers have dug up one technique after another that lets a hacker trick Intel's microprocessors into spilling a computer's deepest secrets. As those flaws have been exposed, chipmakers have scrambled to patch them. But for one serious form of those attacks, it turns out that Intel still hasn't successfully patched the underlying problem despite 18 months of warnings—and not one but two failed attempts to do so."

Greenberg looked at the Intel announcement and explained to readers that Intel would now be issuing "yet another update to its processors designed to solve a problem it calls 'microarchitectural data sampling,' or MDS. Different teams of researchers who independently discovered the issue call it RIDL or Zombieload."

If you are curious about reading up on Microarchitectural Data Sampling, the Intel Developer Zone has a section on it. Intel's discussion said that "First identified by Intel's internal researchers and partners, and independently reported to Intel by external researchers, Microarchitectural Data Sampling (MDS) is a sub-class of previously disclosed speculative execution side channel vulnerabilities..."

What is ZombieLoad? This is a "speculation execution vulnerability," said Allan; It can be worked to exploit flaws in the way Intel's CPUs handle data. Hackers, potentially, could "steal all manner of sensitive information like passwords, browsing history and so forth."

On Jan. 27, Intel's Jerry Bryant had said that Intel confirmed "that some amount of data could still potentially be inferred through a side-channel and would be addressed in future microcode updates. The issues have been referred to by researchers as Zombiload, RIDL, and CacheOut."

Bryant is communications director, Intel Product Assurance and Security.

In his Jan. 27 post, Intel's Bryant said, "Today we released INTEL-SA-00329, Intel Processors Data Leakage Advisory concerning two vulnerabilities that were publicly disclosed by researchers. As part of our commitment to transparency, the advisory has been released before our planned mitigations can be made available and we expect to release mitigations through our normal Intel Platform Update (IPU) process in the near future."

To repeat, the issues have been referred to by researchers as ZombiLoad, RIDL and CacheOut.

There is a patch, then, to fix a couple of variations on the ZombieLoad security flaw.

"Some of the researchers first warned Intel about the more serious of the two flaws that it's trying to fix now in a paper shared with Intel fully a year ago. Other researchers even shared proof-of-concept code with the company last May," wrote Greenberg in *Wired*.

In coming weeks, Intel said it will make available a new update, and this update "is intended to fix two methods to exploit Intel chips via MDS, which have remained possible even after Intel released MDS patches in May of 2019 and then again last November."

Intel has responded to researchers' findings all along the way. Intel's Bryant referred to the two patch events in May and November mentioned earlier here.

Bryant stated that "Since May 2019, starting with Microarchitectural Data Sampling (MDS), and then in November with TAA, we and our system software partners have released mitigations that have cumulatively and substantially reduced the overall attack surface for these types of issues. We continue to conduct research in this area—internally, and in conjunction with the external research community."

The wrinkle for Intel outsiders appears to be in the momentum of response. Greenberg pointed out the time element in being told of the problem and taking action. He wrote that "for one serious form of those attacks, it turns out that Intel still hasn't successfully patched the underlying problem despite 18 months of warnings," plus the two previous failed attempts.

Greenberg explained that the new update to its processors was designed to solve a problem it calls "microarchitectural data sampling," or MDS.

Greenberg quoted a Vrije Universiteit researcher, Herbert Bos. The latter said the fact that Intel left variants of MDS unpatched for more than 18 months raised the question of whether sophisticated hackers may have already used them on real targets.

Intel's recent blog post nonetheless stated that "to date, we are not aware of any use of these issues outside of a controlled lab environment." (*Naked Security*: "To date, exploiting ZombieLoad weaknesses has been viewed as a complex undertaking that had only been shown to work under unusual lab conditions—no attacks exploiting these methods has ever been detected.")

(Bos said that the technique "leaves no trace that would make in-the-wild attacks detectable.")

Naked Security put this MDS focus in perspective, considering the threads that occupy security concerns at Intel:

"The problem that's tying down Intel's patching team these days is a more recent class of side channel vulnerabilities known collectively as ZombieLoad. These relate to a data leakage problem called Microarchitectural Data Sampling (MDS) affecting Intel's speculative execution technology introduced in the late 1990s to improve chip performance. ZombieLoad is also what Naked Security likes to call a BWAIN, or Bug With an

Impressive Name. BWAINs are everywhere with side-channel issues in microprocessor hardware proving particularly good at generating new ones."

Meanwhile, Paul Lilly in *HotHardware* zeroed in on another attack method in the MDS family. This one is CacheOut. Lilly reported that "Intel has worked with its system software partners to push out separate patches and firmware updates for CacheOut." Lilly provided a link to a page that shows a list of potentially affected CPUs.

In the ZombieLoad site researchers posted helpful explanations of ZombieLoad's ways in the FAQ section.

Basically, though, with all the technical details to understand, *Naked Security* wrapped it all up with the news that "the researchers announced they'd dug up more CPU data-extraction holes." The past mitigations had not been enough.

More information:
blogs.intel.com/technology/202 …
-sa-00329/#gs.vfdtqy

APA citation: Intel casts third patch to battle MDS Goliath (2020, January 30) retrieved 28 September 2022 from https://techxplore.com/news/2020-01-intel-patch-mds-goliath.html