Detect security holes in both AMD's Ryzen and Threadripper chips

Most noteworthy is that Intel is a partial sponsor of the security vulnerability research project on AMD chips.

Though it was thought that only Intel chips contain security holes that are difficult to fix when it comes to hardware, but recently researchers at Graz University of Technology described in detail the duo of the sub-channel attack. called Collide + Probe and Load + Reload, can leak confidential data in AMD processors by manipulating the Level 1 cache prediction block.

The cache prediction block is designed to increase the efficiency of cache access in the processor. The researchers claim that this "Take A Way" sub-channel attack affects every AMD processor from 2011 to 2019, meaning that this vulnerability appears on both the Athlon 64 X2 and Ryzen 7 processors. and ThreadRipper.

While the Collide + Probe attack allows an attacker to monitor memory access without knowing the physical addresses or shared memory, the Load + Reload attack is a more secretive approach to using the Use shared memory without disabling the cache stream, allowing an attack to be made without the victim's knowledge.

Unlike other sub-channel attacks, these holes soon show how they will impact the real world. The team exploited this vulnerability by running JavaScript on Chrome and Firefox browsers as well as gaining access to AES encryption keys. This type of exploitation is also used to penetrate clouds in data centers.

Compared to the Meltdown and Specter vulnerabilities on Intel processors, the researchers emphasized that their "Take A Way" exploit only leaked "a few bits of metadata" on the processor. AMD, instead of gaining complete access to the data as it did with the Meltdown flaw.

The researchers also said that this flaw can be handled with a combination of hardware and software, although it is unclear how this will affect performance. Software and firmware patches for Meltdown and Specter vulnerabilities often degrade Intel processor performance, depending on the task being different.

The vulnerability has been reported to AMD since the end of August 2019, but so far researchers have not received a response from the chip designer.

One thing worth noting in this study are the sponsors for it. Besides organizations such as the French National Research Agency, the European Research Council or the Austrian Research Promotion Agency, there is another special name: Intel - AMD's biggest rival on the playing field. x86 processor. The research document also said that Intel has patched a similar hole in the processor.

Refer to Engadget