# AMD CPUs also have security vulnerabilities that have existed for many years now!

Another relatively serious vulnerability on AMD processors has continued to be discovered, prompting the security community.

Just a few days ago, we warned of an 'unpatchable' security hole affecting millions of Intel users around the world. While the information is still not hot, another relatively serious flaw on AMD processors has continued to be made public by the security community.

A group of international security researchers from the University of Technology Graz (Austria) and the University of Rennes (France) have just discovered a vulnerability exists on AMD CPUs, affecting all sets. handle Athlon 64 X2, Ryzen 7 and ThreadRipper produced over a period of 9 years, from 2011 to 2019. This vulnerability directly paves the way for side channel attacks called Collide + Probe and Load + Reload. If successfully exploited, it could allow hackers to access confidential data in AMD processors. The common point of both attacks is that the "prediction tool" is used for level 1 caching (L1 cache) to cause leakage of cached content. The report is given as follows:

*The prediction tool calculates a? Tag using a hash function not stored on a virtual address. ? This tag is used to look up the way to store L1D buffer in the prediction table. Therefore, the CPU must compare the buffer tag only once to reduce power consumption.*

*In the first attack technique, Collide + Probe, an intruder will track memory accesses without having to know the physical address or shared memory area.*

*In the second attack technique, Load + Reload, the hacker exploits an attribute in which physical memory location can only exist once in the L1D buffer. Provides the ability to manipulate shared memory without invalidating the buffer stream.*

*The process of exploiting the flaw can be done through JavaScript code on popular browsers without the victim's knowledge. Although the amount of data collected is not too large, it is enough to detect important AES encryption keys.*


In fact, information about the flaw was alerted by security researchers to AMD in late August 2019, but the company proved passive and didn't issue a firmware update to resolve the issue.

The good news is that this flaw will not lead to large-scale data leak attacks like Meltdown or Zombieload on Intel chips. At the same time, it can be overcome through measures combining hardware and software.

Hopefully, AMD will take actions to express a clearer view of this vulnerability in the near future.