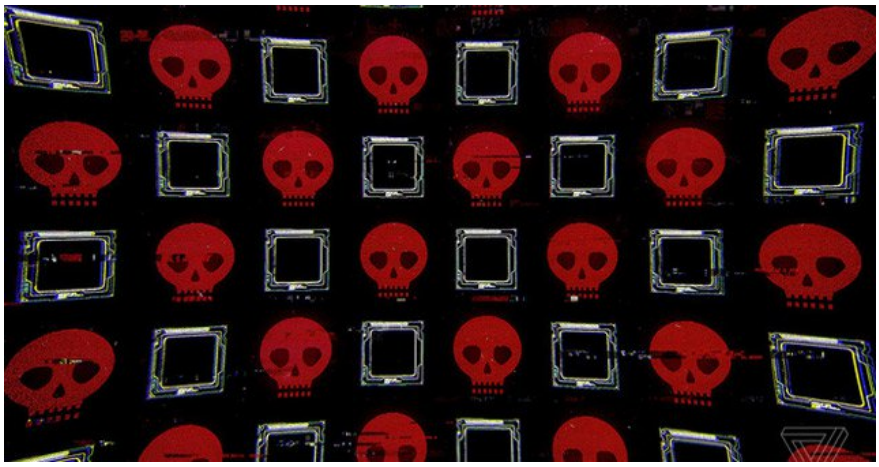
New dangerous vulnerability in Intel CPU: Works like Specter and Meltdown, threatening all PCs and the cloud

An extremely serious new class of Intel chip vulnerabilities has been discovered by security researchers at Graz University of Technology, if successful exploitation of the bad guys can take advantage of it to steal sensitive information online. Next from the processor.

An extremely serious new class of Intel chip vulnerabilities has been discovered by security researchers at Graz University of Technology, if successful exploitation of the bad guys can take advantage of it to steal sensitive information online. Next from the processor.

The new vulnerability is made up of 4 errors and is named "ZombieLoad". It is worrisome that hackers can even take advantage of ZombieLoad on cloud phone servers to do bad purposes.

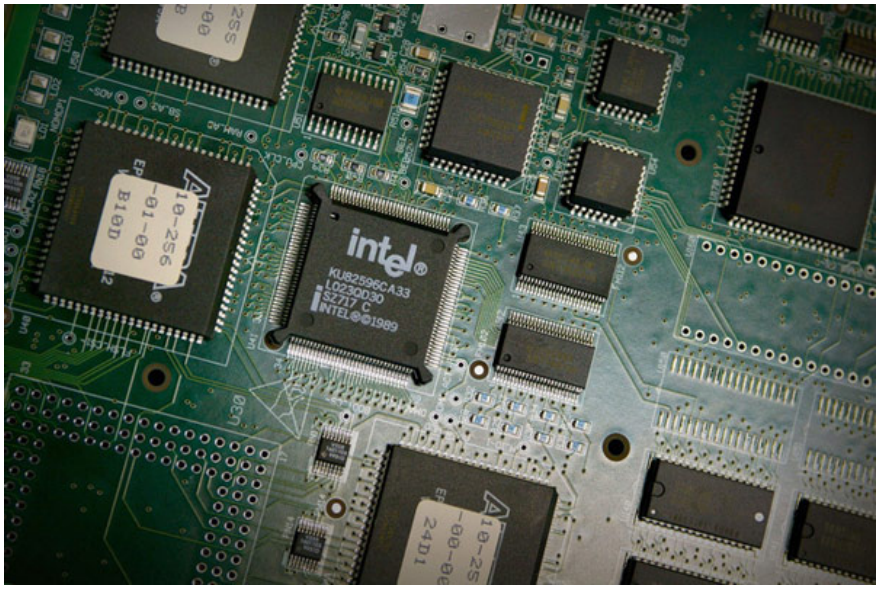


Security researchers discovered ZombieLoad a month ago and immediately told Intel.

Currently, Intel has completed patching the motherboard BIOS to fix this critical error. However, unlike Windows 10 auto-patching, Asus or MSI and other mainboard manufacturers will have to create their own BIOS to match their product line so that users can download it and go to the machine.

This vulnerability affects nearly all computers using Intel chips from 2011 to the present.

Apple and Google have also released new updates to patch Zombieload. Microsoft also said it will release the patch as soon as possible.



Researchers have said that until now, there has been no case where Zombieload has been exploited by a bad person to infiltrate a personal computer.

Not only Zombieload, but in fact there are many serious security errors, taking advantage of the process of running CPU processes that users 'might' need (speculative execution) to increase processing speed. All current CPU generations are integrated with this feature.

In 2018, when researchers discovered Specter and Meltdown, hackers also took advantage of this feature to perform attacks.

Intel said that Zombieload patches will make the CPU slower than before due to the speculative execution feature will be more tightly controlled. Specific performance on personal computers can be reduced by up to 3%, while on data environments can be up to 9%. However, users will not recognize this change.