Intel claims: New security updates help the computer to be 'immune' to Meltdown and Specter

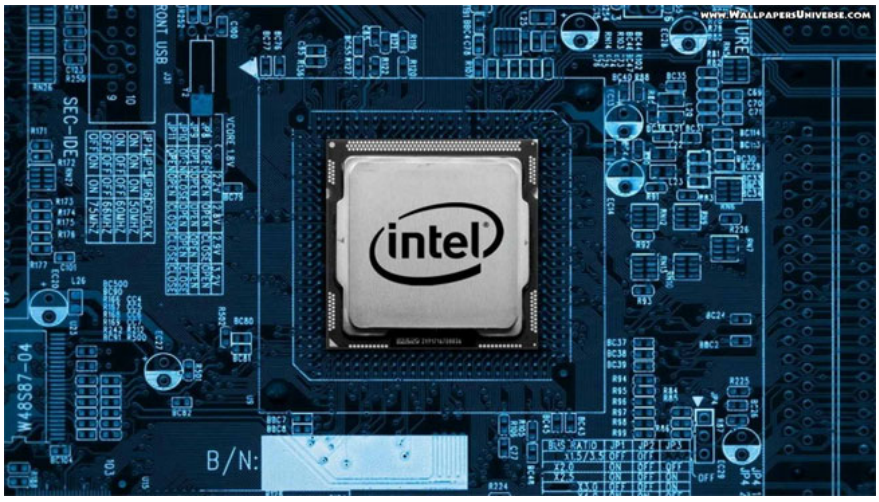
Intel claims that its new security patches will help the computer be immune to two extremely serious security bugs, attracting users' attention during the past two days: Meltdown and Specter. Also in this statement, the company confirmed that by the end of the week, 90% of computers will be protected.

The article is in the series The overview of holes on chips Intel, AMD, ARM: Meltdown and Specter, you can find useful information regarding these two security holes here.

Intel announced that it and its partners have made significant improvements in security patches and software updates to protect users from two serious CPU errors: Meltdown and Specter. These two vulnerabilities were discovered by Google's Project Zero team earlier this week. It is making the entire computer industry struggle to release fixes and device security patches for customers.

Meltdown and Specter affect most devices produced in the last 20 years and allow attackers to use JavaScript code to run on the browser to access memory. Memory contents may contain key strokes, passwords and other valuable information.

Intel said it has developed and released an update for all Intel-based computers, which "will make these systems immune to both security bugs (Meltdown and Specter) by Google. Project Zero detected ". Intel spokesman also said: "Intel has released an update for most of the chips produced in the last 5 years. By the end of next week, Intel is expected to release updates to more than 90% of the chips. Introduced since 2012 by yourself.



Intel's "immune" promise

"immune" in Intel's statement, is an interesting detail. The New York Times reported on January 3, 2018 that the Specter bug fix was much more complicated because it needed to redesign the processor and hardware changes, we might have to live with the threat from Specter exploit exploits in the next few years. Intel's word "immune" means that this error is not the only one they have, as well as the release of security patches that are not solely Intel's responsibility.

Microsoft started rolling out a security patch for Windows 10, an update for Firefox, Chrome will be released later this month. Apple has confirmed that macOS and iOS devices are also affected by these two errors and have implemented a security patch in macOS 10.13.2, expected to be more complete.

While related companies are working urgently to release security patches in time, there has been a lot of discussion around whether Meltdown and Specter patching will slow down the computer. Intel also answered this question: "Intel believes that the impact of patches on computer performance depends very much on the volume of work. For average computer users, the impact is not Significantly, this impact will decrease slightly over time, for certain workloads, the initial impact of the patches will be higher, but then the company will conduct identification, testing and improvement. software update to mitigate that impact ".

For Windows computers, using modern CPUs, there is no significant performance impact yet, but there are still doubts about Linux computers and virtual machines used for cloud computing. . Some Linux administrators are reporting performance implications on their systems.

It is still too early to assess the overall impact of patches on device performance, but with 90% of the chips patched at the end of next week, we will have a more accurate view of the impact. of these patches to performance. Until then, Intel said it would continue to work with partners and stakeholders to address these issues.

See more:

1. How to protect the computer against Meltdown vulnerability on CPU?
2. Windows 10 KB4056892 emergency update (build 16299.192)
3. Apple confirmed that all Mac and iOS devices are affected by Meltdown and Specter