Intel released a new patch to fix the Specter and Meltdown vulnerabilities

Intel has officially released the latest and stable patch for the two Specter and Meltdown vulnerabilities, causing it to restart automatically. This patch is for 6th generation processors (Skylake), 7 (Kaby Lake) and 8 (Coffee lake) including Core i, Core X, Scalable Xeon and Xenon D.

Intel has officially released the latest and stable patch for the two Specter and Meltdown vulnerabilities, causing it to restart automatically. This patch is for 6th generation processors (Skylake), 7 (Kaby Lake) and 8 (Coffee lake) including Core i, Core X, Scalable Xeon and Xenon D.

2 Specter and Meltdown vulnerabilities were discovered by security experts in the design and operation mechanism of many Intel processors. Hackers can take advantage of these two vulnerabilities to attack using JavaScript from the browser.

Many computer manufacturers have now released lfirmware patches, updated via BIOS / UEFI to prevent the risk of attack through these two vulnerabilities.

In January, Intel also released the Specter and Meltdown patch, but quickly received feedback on whether the machine was constantly restarting or could not even start up on multiple processors from old to new. Skylake, Kaby Lake are also not outside the affected list. After that, Intel had to inform the user to stop updating this patch.

This microcode update from Intel was transferred to OEM partners to overcome the previous issues related to the 2 Specter and Meltdown vulnerabilities that are available on the Skylake, Kaby Lake and Coffee Lake lines, equivalent to Core i 6th generation. , 7, 8 and Core X for end users as well as Scalable and Xeon D Xeon used in data centers.

The new microcde will be released by OEM manufacturers as a firmware update (BIOS / UEFI). Users should pay attention to update when the patch is released.

This update is released through OEM manufacturers, so it takes a while for the update to be delivered to users. ASUS computers must wait for ASUS to release a new BIOS / UEFI update for MSI's motherboard or device, and wait for MSI to update. Hopefully this patch will not be as many bugs as the previous patch.

See more:

1. Microsoft released an emergency patch for Windows, turned off the Specter patch, causing a drop in system performance
2. PC with Skylake and Kaby Lake CPUs failed to restart automatically after installing Meltdown & Specter patch
3. How to protect your computer against Meltdown and Specter security errors