How to protect the computer against Meltdown vulnerability on CPU?

As detailed information on two serious security holes on the processor gradually cleared up, companies are trying to release security patches.

This article is in the series: Overview of vulnerabilities on Intel, AMD, ARM chips: Meltdown and Specter. Please read all the articles in the series to get information as well as take steps to protect your device against these two serious security holes.

As detailed information on two serious security holes on the processor gradually cleared up, companies are trying to release security patches.

Named Meltdown and Specter, these two errors affect almost every device produced in the last two decades . Meltdown only on Intel chips and researchers have also released PoC code describing the attack exploiting this error.

The vulnerability allows an attacker to take over the memory process on the processor by exploiting parallel processes. Attackers can use JavaScript code to run on the browser and access the memory of processes on the machine. From there, users can lose many important data.

Researchers have shown that it is easy to attack on Linux, and Microsoft claims there has been no case of exploiting a vulnerability on Windows. The protection of Windows PC so far is not simple because there are many unknowns.

Microsoft, Google and Mozilla both released patches for their browser. Firefox 57, Internet Expolorer and Edge on Windows are all patched. Google will release a patch on Chrome 64, released on January 23. Apple hasn't said specifically about the plan to patch Safari or even macOS. Overall, Chrome, Edge and Firefox users only need to update automatically.

The OS is a bit more complicated. Microsoft has released an emergency security patch via Windows Update, but if you use antivirus software, you may not see it.

There is still a need to update firmware from Intel to protect the firmware and will be released through each OEM separately. Each OEM has its own release plan, with support information, so you should visit their website for details.

Computer protection requires the co-operation of both hardware and software

If you use a Windows PC or laptop, it is best to update to the latest Windows 10 and update BIOS from Dell, HP, Lenovo . Hopefully Microsoft or Intel will release a protection level test tool on both firmware and Windows. Only PowerShell is currently available. Here are some basic steps if you are not used to PowerShell:

1. Update the latest version of Chrome or Firefox.
2. Make sure to install Build KB4056892 on Windows 10 via Windows Update
3. Check the OEM website for support information or firmware updates

The above steps only help protect against Meltdown. Specter is still unknown and security experts say it is also harder to exploit than Meltdown. Specter fix is ??also more complicated because of the need to redesign the processor and hardware changes. So maybe we will have to live with Specter for a few more years.

Please download the browser patches below.

1. Firefox 57: *https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/*
2. Internet Explorer and Edge: *https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/#tpOa1SwmRDKibAxg.97*
3. Check security vulnerabilities with PowerShell: *https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in*

See more:

1. Apple confirmed that all Mac and iOS devices are affected by Meltdown and Specter
2. All you need to know about Meltdown and Specter - two dangerous vulnerabilities are present on billions of devices running Intel, AMD and ARM chips.
3. Serious security vulnerability on Intel chips