How to know if your Windows computer is affected by Meltdown and Specter?

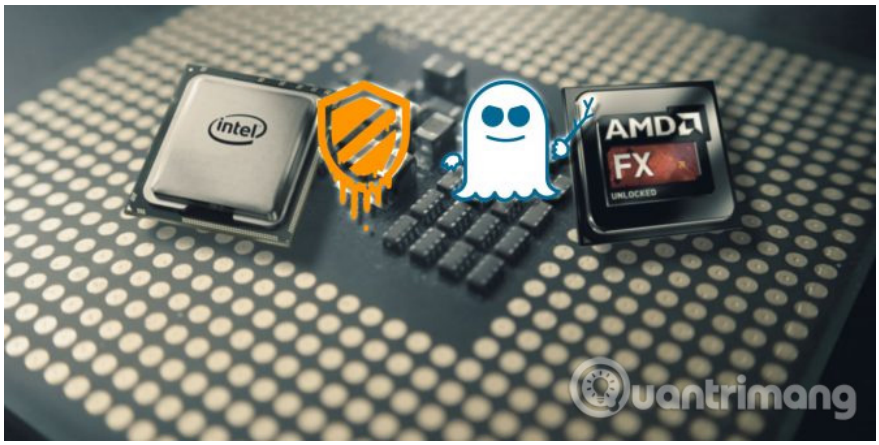
How to know if your Windows computer is affected by Meltdown and Specter? Let TipsMake.com learn more about the extent of the impact of the vulnerabilities and whether they affect your computer or not in this article!

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.

1. How slow is Meltdown and Specter, which is Microsoft's explanation
2. How to protect your computer against Meltdown and Specter security errors
3. Intel will fix Meltdown and Specter over 90% of new products within 1 week

New year means a new beginning. 2017 has brought us many security issues such as the WannaCry ransomware and **Equifax hack** but everything is not better than this in early 2018.

We have just finished welcoming the new year, a security "bomb" has appeared on a series of newspaper pages. Not a hole, but two holes at the same time. Their nicknames are **Meltdown** and **Specter** , they are found on computer processors. In terms of severity and the number of people who could be affected, experts compared them to Heartbleed errors in 2014. (*Heartbleed is a very serious error (CVE-2014-0160) of the OpenSSL encryption library, which occurs when deploying more OpenSSL TLS and DTLS heartbeat expansion features.*)



Meltdown and Specter can affect all desktop operating systems, but in this article, we only focus on the Windows operating system. We learn more about how these vulnerabilities affect them and whether they affect your computer.

If you don't know anything about Meldown and Specter then make sure you haven't missed the article: All you need to know about Meltdown and Specter - 2 dangerous vulnerabilities are present on billions of devices running Intel, AMD, ARM

Is your Windows computer affected by Meltdown and Specter?

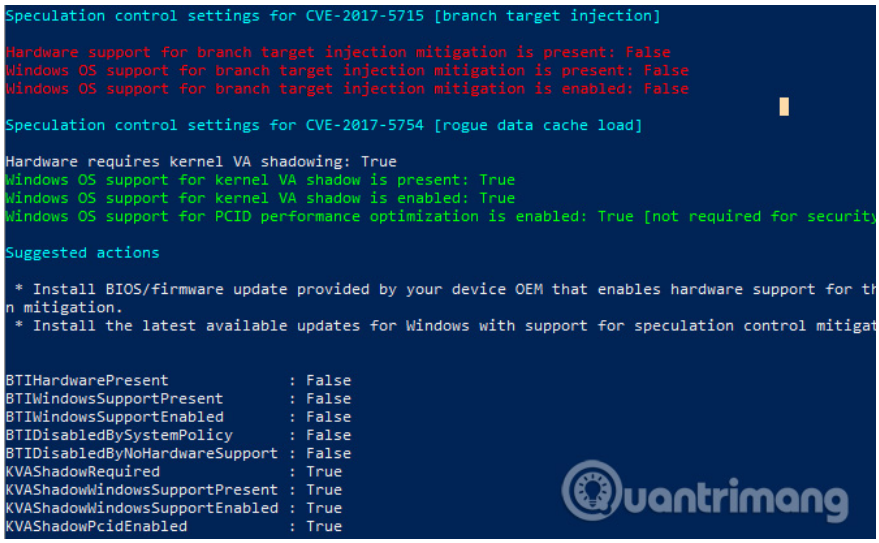
You need to assume you are affected by Specter and you can overcome this.

But what about Meltdown security vulnerabilities? Thankfully, Microsoft exported a handy PowerShell script that you can run on the system. Follow the steps below to **install and activate an additional module on the system** . The result will indicate whether you need to take further steps or not.

First, run PowerShell as an administrator: press the **Windows + Q** key or open **Start Menu** , type **PowerShell** , right-click the first result (Windows PowerShell, the desktop application) and select **Run as administrator** .

After PowerShell has been downloaded, follow these steps to find out if your computer is affected by Meltdown. **Note** : You can copy and paste commands into PowerShell.

1. Enter **Install-Module SpeculationControl** and press **Enter** to run the command.
2. Confirm the prompt of the NuGet provider by entering the **Y** key for Yes and clicking **Enter.**
3. Do the same with unreliable archive reminders.
4. When the installation is complete, enter **Import-Module SpeculationControl** and press **Enter** .
5. Finally, type **Get-SpeculationControlSettings** and press **Enter** .



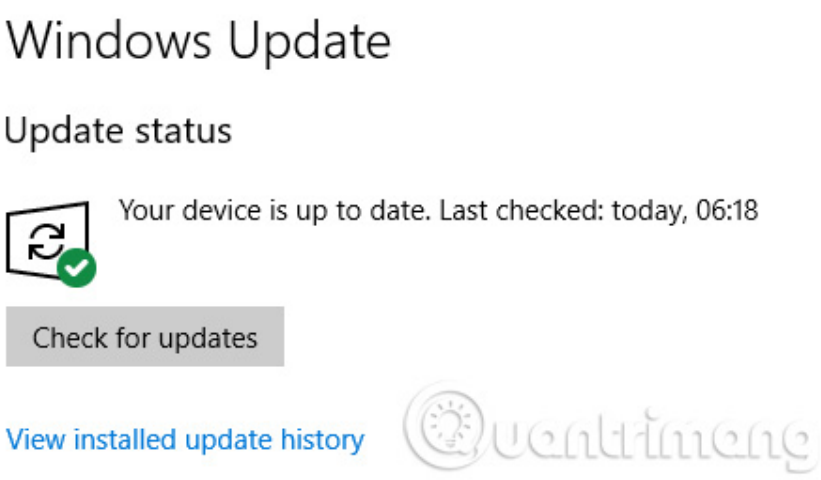
After running these commands, check the output - **True** (True) or **False** (False).

If you only see **True** messages, congratulations, you are protected and do not need to take any further action. If any False message appears, your system will be vulnerable to attack and you need to take further action. Please make sure the suggested actions are displayed in the results. As shown on the screen above, our test computer requires **BIOS / firmware update** and has not installed a patch provided via Windows Update.

1. Instructions for upgrading BIOS

How can you protect your computer?

Want to hear good news or bad news first? The good news is that you **can protect your computer from Meltdown security vulnerabilities** . The bad news is that it is not a permanent solution and your computer will lose performance. And another bad news is that **you can't protect yourself from the Specter security hole** .



Microsoft quickly released a patch for Meltdown. You can find it through the Windows Update tool (**Settings**)> **Update & Security** > **Windows Update** > **Check of updates**). You need to download and install the KB4056892 patch for Windows build 16299.

Note: Microsoft patch, Intel for these two vulnerabilities currently (on 17/1/2018) still cause errors such as blue screen, unstable operation on Windows, you should not temporarily update.

1. Windows 10 KB4056892 emergency update (build 16299.192)

Note that the patch is not compatible with some antivirus suites. It only works if your security software provider has updated **ALLOW REGKEY** in the Windows registry.

Besides, you should also update your browser. Google patched Meltdown in Chrome 64 and Mozilla updated Firefox in version 57. Microsoft even patched the latest version of Edge. Check your browser developer if you use an unofficial application.

Finally, you need to update the system BIOS and firmware. Some computer manufacturers including a Windows application can quickly check for those updates. If the manufacturer of your computer does not provide it or if you have deleted it, you can find updates on the manufacturer's website.

1. How to set up BIOS to boot from USB / CD / DVD, external hard drive

About Specter security hole?

Of course this will not be a satisfactory answer for many people, but the current advice is CAREFULLY. Meltdown is a direct threat and is one of two easy errors for hackers to exploit.

Because of the way Specter works, fixing it will require manufacturers to completely redesign the way to build the processor. This process can take years and probably decades until the current processor is completely non-circulating.

With the number of devices affected - possibly billions - a recall notice is impossible. We will have to live with the threat of a Specter attack for years to come.

Do Meltdown and Specter vulnerabilities make you feel nervous?

It's easy to understand when all of us feel anxious. After all, computers are holding the "key" to our modern technology life.

However, it is also important to get comfort from reality. You will not be the victim of Specter attack. The time and effort a hacker needs to achieve an unspecified return makes you an unattractive proposition.

And the big tech companies have known these two issues of security vulnerabilities since mid-2017. They have had plenty of time to prepare patches and respond in the best way they can.

Despite the fact, the threats of Meltdown and Specter still make you feel anxious, right? Please let us know your thoughts and opinions in the comment section below!

Refer to some more articles:

1. Overview of vulnerabilities on Intel, AMD, ARM chips: Meltdown and Specter
2. How to protect the computer against Meltdown vulnerability on CPU?
3. Microsoft's patch of Meltdown and Specter makes Windows Phone unstable, causing a blue screen error on the PC

Having fun!