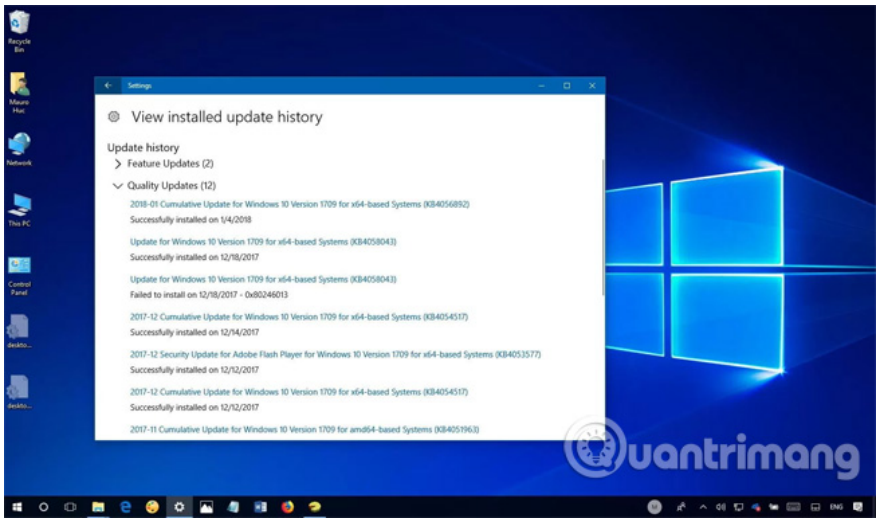
How to protect your computer against Meltdown and Specter security errors

Let's TipsMake.com find out the details of the steps to perform computer protection before Meltdown and Specter security errors in this article!

1. Find security holes on every site with Nikto
2. Microsoft silently patched the KRACK WPA2 security hole
3. Microsoft released an emergency security patch for a serious vulnerability

Let's TipsMake.com find out the details of the steps to perform **computer protection before Meltdown and Specter security errors** in this article!

Recently, it has been revealed that most modern processors released in the last 20 years have security holes. These security bugs are known as " **Meltdown** " and " **Specter** ". Basically, they allow malicious software **to steal personal data** (for example, passwords, encryption keys, browser history, documents, emails) stored in the central memory area covered. Protect on your device.



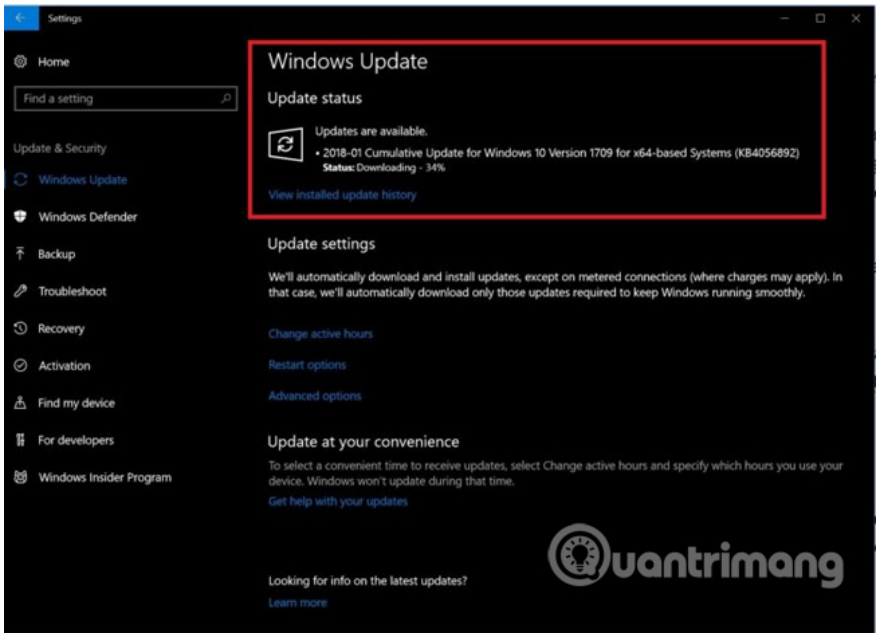
These are hardware-level errors and affect most modern processors, including processors from Intel, AMD and ARM - but Intel's processors are "vulnerable." "More because AMD said that some vulnerabilities do not affect their chips. In addition, this also affects versions of Windows as well as Linux, macOS, Google OS and other operating systems.

Unfortunately, these are the internal flaws in the processor design and cannot be modified through software updates. However, hardware and software vendors can update their software to minimize problems. This solution comes with a performance reduction, that fixes will make your computer up to 30 percent slower

depending on the processor model.

If you are using a personal computer, keeping it safe at this time is not easy, because they are still in the early stages and there are many pieces. But there are some things you can do to protect your device.

Install the latest update of Windows



If you use Windows 10, Microsoft has provided an emergency patch for all Windows versions, which is part of a series of updates to address these vulnerabilities.

The Windows 10 1709 version (Fall Creators Update) received the KB4056892 update, while version 1703 (Creators Update) received the update KB4056891.

Older versions of the operating system will also be patched:

1. KB4056890 - Windows 10 1607 version (Update Anniversary Update version)
2. KB4056888 - Windows 10 version 1511 (November update)
3. KB4056893 - Windows 10 version 1507 (Initial version)

The update will automatically download and install, but you can also update yourself on **Settings** > **Update & Security** > **Windows Update** and click the **Check for updates** button.

To check if your device is protected, go to **Settings** > **Update & Security** > **Windows Update** , click the link **View installed update history** (See history). installed) and ensure "Quality update", the latest update has been applied.

Windows 8.1 and Windows 7 will also receive an update that protects the computer from these vulnerabilities, and users running older versions of Windows will not receive updates until Tuesday.

Note that Microsoft has quietly patched the beta version of Windows 10 available through the Insider program.

Set up manual updates

If your device does not update itself, it may be due to an issue with Windows Update or an antivirus program that has not been upgraded to support the latest update.

Recently, Microsoft noted the problem that some antivirus software is trying to communicate with central memory using unsupported calls and this behavior causes a check bug - often called a **Screen.** Blue Screen of Death (Blue Screen of Death)

To prevent devices from having this problem, Windows Update will not install the latest fixes but has installed an unpatched antivirus solution.

In addition, you can solve this problem by uninstalling a third-party antivirus program and using Windows Defender Antivirus until the software vendor issues an update.

Update the firmware

In addition to ensuring that all software is up to date, you should also regularly monitor your computer manufacturer (eg HP, Dell, Lenovo, Asus) to update new software.

Intel has begun offering bug fixes to solve the Meltdown and Specter security bugs on devices that use their processors. Microsoft has just released a firmware update to protect the Surface device against these security errors.

Update the entire software

In addition, you need to make sure that the applications in your computer are also updated. According to Mozilla, Firefox 57 has a fix, Microsoft has updated Microsoft Edge and Internet Explorer.

Google is expected to release a fix with Chrome 64 on January 23, but for now, you can enable Site Isolation site isolation on Chrome during your own use to supplement it. add a layer of protection.

1. How to enable Site Isolation security feature on Chrome

Summary

If you are using a Windows-based computer, what to do at this time is to make sure Windows 10 has the latest updates and BIOS or UEFI updates. In addition to the above suggestions, there is nothing you can do to protect your device against Meltdown and Specter vulnerabilities.

Refer to some more articles:

1. Serious security vulnerability on Intel chips
2. AMD and ARM both warned of security flaws like Intel processors
3. How to protect the computer against Meltdown vulnerability on CPU?

Having fun!