How to protect your computer against a Foreshadow security vulnerability

Foreshadow is a security error that allows malware to enter secure areas of the computer.

What is Foreshadow?

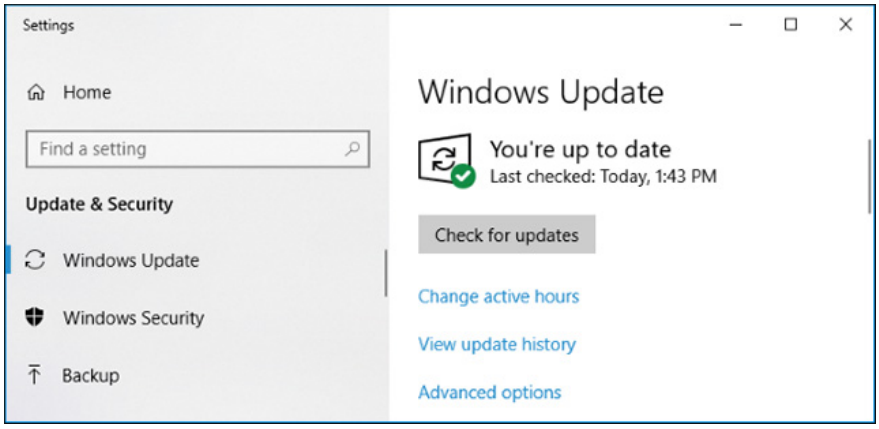
Foreshadow, also known as L1 Terminal Fault, is a security bug thataffects one of Intel's security elements (Software Guard Extensions (or SGX)..It allows malware to enter secure areas that even the previous security holes of Specter and Meltdown cannot break.

Specifically, Foreshadow attacked Intel's software protection utility (SGX) feature.This feature is integrated into Intel chips to allow programs to create "zones" safe that even other programs on the computer cannot be accessed.In addition, in theory, even if malware enters the computer, it cannot access these secure areas.When Specter and Meltdown security bugs were released, security researchers found that the memory protected by SGX was virtually unaffected by Specter and Meltdown.

Foreshadow has two versions: the initial attack is to retrieve data from the safe area of ??SGX and the second is Foreshadow NG (Next Generation) to retrieve information in the L1 cache.NG affects both virtual machines, OS kernel memory, system management memory, potentially threatening the entire cloud platform architecture.

You can find out more about this vulnerability here:Foreshadow - the fifth most serious security vulnerability on the CPU in 2018

How to protect your PC before Foreshadow



Note that only Intel-based computers are susceptible to attack by Foreshadow.AMD chips rarely get this security error.

According to the official security advice from Microsoft, most Windows-based PCs just need to be updated to the operating system can protect themselves from Foreshadow.Just run Windows Update to install the latest patches.Microsoft also said it did not notice any impact on the performance of the machine after installing these patches.

Some PCs may also neednew microchips fromIntel to protect themselves.Intel said these are thesamemicrocodeupdatesthat were released earlier this year.It is possible to obtain a new firmware update, by installing the latest UEFI or BIOS update from either your PC or motherboard manufacturer.In addition, it is also possible to installthe microcodeupdatedirectly from Microsoft.

Notes for system administrators

For PCs running hypervisor software for virtual machines (for example, Hyper-V) that hypervisor software will also need to be updated to the latest version.For example, in addition to the Microsoft update for Hyper-V, VMWare has also released updates for their virtual machine software.

Systems that use Hyper-V or other virtualization-based security platforms will also need stronger changes.Including disabling hyperthreading, this will slow down the computer, and of course most people will not need to do this, but for Windows Server administrators running Hyper-V on Intel's CPU, they will need to seriously consider disabling hyperthreading in the system BIOS to keep their virtual machines safe.

Cloud utility vendors such as Microsoft Azure and Amazon Web Services are also actively running patches for their systems to avoid being attacked by virtual machines on these data-sharing systems.

Other operating systems also need to be updated with new security patches.For example, Ubuntu has released a new update to protect Linux machines before these attacks.While Apple has not yet made any formal moves.

After identifying and analyzing CVE data, the security has identified the following errors: CVE-2018-3615 to attack Intel SGX, CVE-2018-3620 attack on the operating system and mode System management and CVE-2018-3646 to attack the management of virtual machines.

In a blog post, Intel said it is actively working to come up with better solutions as well as improve performance while speeding up blocking L1TF effects.These solutions will only be applied when necessary.Intel said thatthe

microcodefor CPUs previously released by the company has provided this feature to some partners and its performance is still being evaluated.

Finally, Intel noted that L1TF issues will also be addressed by the firm with changes made to the hardware.In other words, future Intel CPUs will bring in hardware enhancements to improve the efficiency of fighting Specter, Meltdown, Foreshadow and other similar attacks and minimize losses. to a minimum.

See more:

1. 17 clear signs that your computer has been attacked by a virus
2. 10 best free antivirus software for computers
3. These "hack" tips are only Notepad can do
4. How do I know if someone has accessed and used your computer?