Detecting a Thunderbolt flaw allows a hacker to steal system data for 5 minutes

Recently, international security researcher Bjorn Ruytenberg unexpectedly discovered a vulnerability called 'Thunderspy' that exists in Thunderbolt ports, allowing hackers to easily steal data.

Thunderbolt is a great achievement when it comes to wired connectivity technology on electronics. This is a high-speed connection standard, developed by Intel under the code name Light Peak and first appeared on the MacBook Pro 2011. The strength of Thunderbolt lies in its ability to both charge and connect. connect and transfer data between computers and other peripherals, all with a single cable. Especially, the ability to transfer data very fast, up to 10Gbps / s - about 2 times higher than USB 3.0 and 20 times higher than USB 2.0. However, Thunderbolt also contains a "fatal" flaw.

Thunderbolt port

Recently, international security researcher Bjorn Ruytenberg unexpectedly discovered a vulnerability called 'Thunderspy' that exists in Thunderbolt ports, allowing hackers to easily steal data stored on the system. if there is physical access to the device, even if the user has a computer key and encrypted data. More seriously, the whole process of exploiting this vulnerability takes only a maximum of 5 minutes to proceed in the case of skilled hackers, and the necessary equipment is just screwdrivers and another "mobile hardware". .

Here is the whole process of Bjorn Ruytenberg's 5-minute Thunderspy flaw exploitation:

The underlying cause of Thunderspy is that Thunderbolt allows external devices to directly access the memory of the PC to retrieve data in a short time. However, a good hacker can intervene directly with the hardware system that controls the Thunderbolt port to connect the PC to other unknown removable devices to steal data. The only downside to this type of attack is that hackers are forced to have physical access to your PC, but it

possesses three other great advantages, which are to leave no trace. can be done in a fraction of the time, and are cheap.

Intel has confirmed Thunderspy's existence, and has implemented a new security system called Kernel Direct Memory Access (DMA) to mitigate and prevent attacks from this vulnerability. However, at the present time, DMA has only been implemented on Windows 10 from version 1803 RS4 and above, Kernel Linux from 5.x and above and MacOS 10.12.4 and above.

As recommended by Bjorn Ruytenberg, users should disable the Thunderbolt ports in the BIOS to completely prevent this vulnerability. You should also keep an eye on your PC and deploy hard drive encryption.