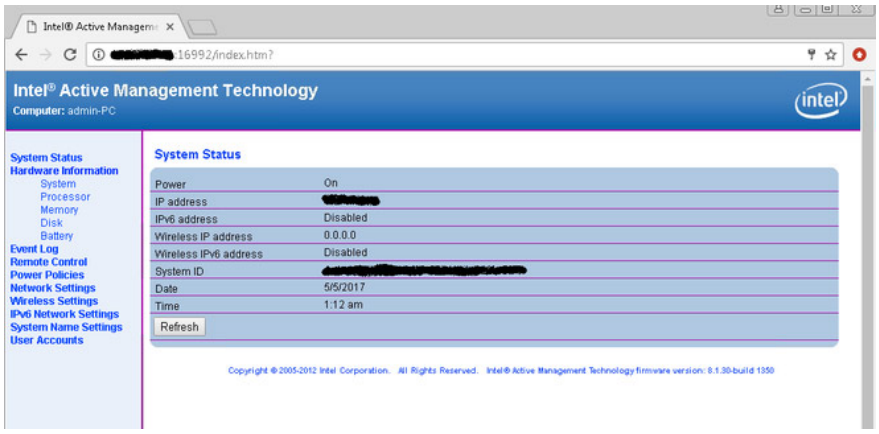
The new vulnerability on Intel allows hackers to take control of your computer within 30 seconds

While Intel's Meltdown and Specter vulnerabilities have not been completely overcome, the world faces a new security vulnerability that allows hackers to take complete control of the user's device and attack time within 30 seconds.

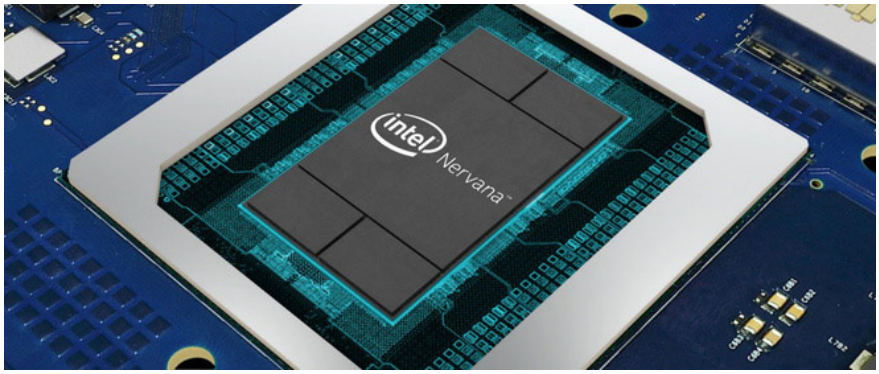
While Intel's Meltdown and Specter vulnerabilities have not been completely overcome, the world faces a new security vulnerability that allows hackers to take complete control of the user's device and attack time within 30 seconds.

Recently, security firm F-Secure, has discovered a new security breach in Intel's remote management technology, Active Management Technology (ATM), which allows hackers to bypass the login screen and security mode.

To improve the administrator's ability to manage and repair computers, workstations and remote servers, Intel chips use a technology called Intel Active Management Technology (AMT). Administrators can access the remote system using a control panel in the form of a Website accessible via port 16992 and 16993. Intel AMT web interface operates independently of the operating system, so the device only needs the device. There is still a power connection and the network connection is still running even if the system is off.



With this vulnerability, any security measure, no matter how strong, can be overcome by hackers. Hackers only need to access the BIOS of the device, change the option to choose Management Engine BIOS Extension (MEBx) and enter "admin" as the password. At that time, all security features will be turned off and only need 30 seconds and some simple actions the hacker can attack the victim's device without spending any code.



This is not the first time security experts have discovered vulnerabilities in AMT. Intel has been notified of this vulnerability, and in order to protect the device before receiving a fix, you should not leave the computer for too long without supervision, but also need to set a password for security technology. AMT in BIOS.

See more:

1. How to know if your Windows computer is affected by Meltdown and Specter?
2. Intel: After installing Specter / Meltdown vulnerability patch your computer will slow down to 10%
3. Intel released Microcode for CPU Linux to fix Meltdown and Specter

You finished reading the article "**The new vulnerability on Intel allows hackers to take control of your computer within 30 seconds**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
