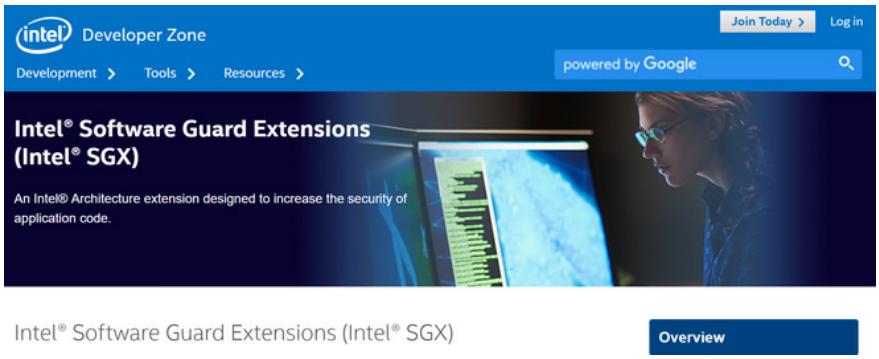
The new Specter vulnerability appears to be a new variant that easily 'crashes' secure partitions created by Intel SGX

Researchers from the Ohio State University have discovered a new dangerous variant of the Specter vulnerability called SgxPectre with the ability to exploit information from safe partitions created by Intel SGX.

Researchers from the Ohio State University have discovered a new dangerous variant of the Specter vulnerability called SgxPectre with the ability to exploit information from safe partitions created by Intel SGX.

Two Specter and Meltdown security vulnerabilities appeared in early 2018, negatively affecting the entire launch process from 1995 to the present. Soon, Intel's new processors were equipped with Software Protection Utility (SGX) to deal with these two security holes.



SGX creates secure partitions for operating software. They are created based on specific needs and own separate memory completely separate from other system software such as operating system or Hypervisor (software responsible for running multiple virtual machines on the same system) to avoid hackers taking advantage of Specter / Meltdown to exploit information on user computers.

But it seems that the hardware-safe partitions created by SGX cannot prevent SgxPectre. It takes advantage of predicting SGX's own actions to steal protected information.

Intel's representative said that shortly after receiving the Ohio University report, the company announced it would release an update package of software development tools for SGX application developers - expected to launch. on March 16 to solve Specter, Meltdown as well as other variants.

At the same time, Intel also recommends that users should use the latest updates of this toolkit.

See more:

1. Microsoft and Intel cooperated to provide microcode updates for the CPU via Windows updates
2. Bkav released a free detection tool for Meltdown and Specter
3. How to block Specter Variant 2 Patch on Windows 10
4.