Frequent vulnerabilities and high failure rates should be used to troubleshoot Intel product network security risks

China Cyberspace Security Association October 16, 2024 11:02

Frequent vulnerabilities and high failure rate
Intel product network security risks should be systematically investigated

1. Frequent security breaches

In August 2023, Intel CPUs were exposed to have a Downfall vulnerability. This vulnerability is a CPU transient execution side channel vulnerability that uses the Gather instruction in its AVX2 or AVX-512 instruction set to obtain the key previously stored in a specific vector register buffer. Sensitive data such as user information and key parameters. The vulnerability affects Intel's 6th to 11th generation Core, Celeron, and Pentium series CPUs, as well as 1st to 4th generation Xeon processors. In fact, as early as 2022, a researcher reported the vulnerability to Intel, but Intel neither acknowledged nor took effective action even though it knew that the vulnerability existed, and continued to sell products with the vulnerability until the vulnerability was discovered. It was publicly reported that Intel was forced to take measures to fix the vulnerability. Five victims have launched a class action lawsuit against Intel in November 2023 at the San Jose branch of the U.S. Federal District Court for Northern California in the name of themselves and representatives of "CPU Consumers across America" in response to the above situation.

Coincidentally, in November 2023, Google researchers disclosed that Intel CPUs have a high-risk vulnerability, Reptar. By exploiting this vulnerability, attackers can not only obtain sensitive data such as personal accounts, card numbers, and passwords in the system in a multi-tenant virtualized environment, but can also cause the physical system to hang or crash, causing a denial of service to other systems and tenants it hosts. Phenomenon.

Since 2024, Intel CPUs have exposed vulnerabilities such as GhostRace, NativeBHI, and Indirector. Intel's major flaws in product quality and security management indicate its extremely irresponsible attitude towards customers.

2. Poor reliability and ignoring user complaints

Starting from the end of 2023, a large number of users have reported that crashes will occur when playing specific games using Intel's 13th and 14th generation Core i9 series CPUs. Game manufacturers have even added pop-up processing to the game to warn users using these CPUs. Dylan Browne, the Unreal Engine supervisor and visual effects lead at visual effects studio ModelFarm, posted that the failure rate of his company’s computers using Intel processors is as high as 50%.

In the face of intensive user feedback that could not be concealed, Intel finally had to admit that the product had stability problems and issued a so-called preliminary investigation report, blaming the problem on the motherboard manufacturer setting too high a voltage. But it was immediately refuted by the motherboard manufacturer, saying that the motherboards it produced were developed according to the BIOS program based on the data provided by Intel, and the cause of the crash did not lie with the motherboard manufacturer. In July 2024, Intel issued a statement explaining the frequent CPU crashes, admitting that due to incorrect microcode algorithms issuing excessive voltage requests to the processor, some 13th and 14th generation processors were unstable. Phenomenon.

Frequent crashes occurred at the end of 2023. It was only half a year later that Intel identified the problem and provided an update procedure, and the mitigation measures provided within half a year were ineffective. This fully reflects that Intel is not actively and frankly facing the defects of its own products. The problem is blind indifference, prevarication and delay. Some professionals speculate that the fundamental reason is that Intel actively sacrifices product stability in order to improve performance and regain competitive advantage. It is also reported that the US law firm "Abington Cole + Ellery" has begun investigating the instability of Intel's 13th and 14th generation processors and will file a class action lawsuit on behalf of end users.

3. Monitoring users under the guise of remote management

Intel, together with HP and other manufacturers, jointly designed the IPMI (Intelligent Platform Management Interface) technical specification, claiming to monitor the physical health characteristics of the server. Technically, the server is managed and controlled through the BMC (Baseboard Management Controller) module. The BMC module allows users to remotely manage devices, enabling functions such as starting the computer, reinstalling the operating system, and mounting ISO images. This module has also been exposed to high-risk vulnerabilities (such as CVE-2019-11181), causing a large number of servers around the world to face great security risks of being attacked and controlled.

In addition, Intel also integrates third-party open source components with serious vulnerabilities into its products. Take the Intel M10JNPSB server motherboard as an example. This product supports IPMI management and is currently out of service. The last firmware update package was released on December 13, 2022. Analysis shows that its web server is lighttpd and the version number is 1.4.35, which is actually 2014. version on March 12, 2011, and the latest version of lighttpd at that time had been upgraded to 1.4.66. There was a 9-year gap between the two. The time span was surprisingly large. This irresponsible behavior puts the network and data security of the majority of server users at huge risk.

4. Hidden backdoors jeopardize network and information security

The autonomous running subsystem ME (Management Engine) developed by Intel has been embedded in almost all Intel CPUs since 2008. It is part of its vigorously promoted AMT (Active Management Technology), allowing system administrators to perform tasks remotely. As long as this function is activated, you can remotely access the computer regardless of whether the operating system is installed. Based on peripheral redirection technology such as optical drives, floppy drives, and USB, it can achieve the effect of physical-level contact with the user's computer. Hardware security expert Damien Zammit pointed out that ME is a backdoor that can fully access memory, bypass operating system firewalls, send and receive network packets without the operating system user being aware of it, and users cannot disable ME. Intel AMT (Active Management Technology) implemented based on ME technology was exposed to have a high-risk vulnerability (CVE-2017-5689) in 2017. An attacker can bypass the authentication mechanism and log in directly by setting the response field in the login parameters to be empty. system, gaining the highest authority.

In August 2017, Russian security experts Mark Ermolov and Maxim Goryachy used reverse engineering to find a hidden switch suspected to be set by the NSA (U.S. National Security Agency). The switch was located in the HAP bit in the PCHSTERP0 field, but this time the flag was not officially listed. recorded in the document. What’s dramatic is that HAP, which stands for High Assurance Platform, is a project initiated by the NSA to build a next-generation security defense system.

If the NSA directly shuts down the ME system by turning on the HAP bit hidden switch, and at the same time, other Intel CPUs around the world run the ME system by default, this is equivalent to the NSA being able to build an ideal where only it has protection and everyone else is "streaking" Monitor the environment. This poses a great security threat to the critical information infrastructure of countries around the world, including China. At present, the software and hardware on ME are closed source, and its security mainly relies on Intel's unilateral commitment. However, facts show that Intel's commitment is weak and unconvincing. The use of Intel products poses serious risks to national security.

5. It is recommended to initiate a network security review

According to reports, nearly a quarter of Intel's global annual revenue of more than US$50 billion comes from the Chinese market. In 2021, Intel's CPUs accounted for about 77% of the domestic desktop market and about 81% of the notebook market; in 2022, Intel's x86 server market share in China was about 91%. It can be said that Intel has made a lot of money in China, but the company continues to do things that harm China's interests and threaten China's national security.

Previously, the US government passed the so-called "Chip and Science Act" to unreasonably exclude and suppress China's semiconductor industry. Intel Corporation is the biggest beneficiary of this act. Intel CEO Pat Kissinger successfully tied Intel to the U.S. government and became the largest partner company in the U.S. chip strategy. It not only received $8.5 billion in direct subsidies, but also received $11 billion in low interest rates. loan.

In order to please the U.S. government, Intel has actively suppressed China on so-called Xinjiang-related issues, requiring its suppliers not to use any labor or purchase products or services from the Xinjiang region. In its financial report, it even compared Taiwan Province with China and the United States. , Singapore, and also took the initiative to cut off supplies and services to Chinese companies such as Huawei and ZTE. This is a typical example of "picking up the bowl to eat, and putting down the bowl to smash the pot."

It is recommended to launch a network security review of Intel products sold in China to effectively safeguard China's national security and the legitimate rights and interests of Chinese consumers.