Hardware Vulnerability Research

CYBR3020

Vulnerabilities and Exploits

Arr Domingo

Student ID: 200458099

Instructor: Clayton Amelia

Table of Contents

Introduction

Hardware Vulnerability refer to weaknesses or flaws in the physical components of computing devices, such as processors, memory, and firmware. It has emerged as a critical concern in the rapidly evolving cybersecurity landscape. Unlike software vulnerabilities, which can often be patched or updated, hardware vulnerabilities are more challenging to address because they are literally part of the physical machine. One of the most common hardware vulnerabilities is Meltdown.

What is Meltdown

With CVE-2017-5754, Meltdown is a vulnerability that leverages the *speculative or out-of-order execution* capabilities of modern Intel CPUs, also known as Rogue Data Cache Load (RDCL) or variant 3 of the CPU speculative execution flaws. This hardware vulnerability works on personal computers, mobile devices, and in the cloud. Every Intel processor which implements out-of-order execution is potentially affected by Meltdown. This vulnerability is the result of a serious design flaw in the affected chips, and the discovery of this issue has led to a redesigning of Windows, Mac, and Linux operating system to mitigate vulnerability and prevent attackers from exploiting it.

On January 3, 2018, Meltdown was publicly disclosed by researchers at Google's Project Zero which is a team that's dedicated to finding security flaws before they can be exploited by attackers. As a result of this discovery, security teams at major tech companies like Apple, Intel,

and Microsoft, as well as open-source Linux developers are now dedicating heavy resources to try and ensure that their processors and operating systems are secured ahead of any malicious exploits.

How meltdown works

Meltdown is a vulnerability created in the execution of a special low-level code called "*kernel code*", which runs specifically during a process known as *speculative execution*.

What is speculative execution / out-of-order execution

As an analogy, imagine a hiker lost in the woods who comes across a fork in the trail creating two roughly parallel paths; one path will get the hiker home, the other will not. Rather than waste time waiting for another hiker to give her directions, she chooses the path she believes is most likely to get her home. At some point on the hike, she comes across a trail marker, if that trail marker informs her that she's on the right path, then she continues down that path and gets home. If the trail marker tells her she is on the wrong path, she quickly backtracks and hops over to the alternate trail, which leaves her no worse off than if she was still at the base of the trail hoping for directions.

Many modern processors perform a similar technique called speculative execution, where the CPU tries to guess what code needs to be executed next, and then performs that code before being required to do so. If the executed code turns out not to be needed, the changes are reverted. This is meant to save time and speed up performance.

Reports on the Meltdown vulnerability are suggesting that Intel CPUs may be performing speculative execution of code without requiring important security checks. It may be possible to write software designed to check if the processor has completed an instruction that would normally be blocked by these security checks. This mishandling of speculative execution creates a CPU vulnerability which an attacker can exploit to access very sensitive data in kernel memory such as passwords, encryption keys, personal photographs, emails, etc.

What is a kernel

A kernel is the program at the core of a computer's operating system. It has complete control over the operating system and administers everything from start-up to the handing of memory. The kernel is also responsible for sending data-processing instructions to the CPU (Central Processing Unit). Most CPUs are constantly shifting back and forth between kernel mode and user mode.

In kernel mode, the CPU is executing code that has unrestrained access to the computer's hardware and memory. This mode is generally reserved for the lowest-level and most trusted operations. Crashes that occur while the CPU is in kernel mode are potentially catastrophic; they can crash the entire Operating System.

What is/was vulnerable

According to Google, every device with an Intel processor chip made after 1995 is affected by Meltdown. Desktop, laptop, and cloud computers which implements out-of-order execution

or speculative execution is potentially at risk. ARM chips (e.g. Cortex-A75) were partially affected while AMD CPUs were mostly immune as their memory permission checks happen before speculative execution touches protected memory. Ideally, the issue is the property of CPU microarchitecture, not of a single OS or application.

Also affected are cloud providers which use Intel CPUs and Xen PV as virtualization without having patches applied. Furthermore, cloud providers without real hardware virtualization, relying on containers that share one kernel, such as Docker, LXC, or OpenVZ are affected.

With Meltdown vulnerability, attackers could read any kernel memory that was mapped into a user process's address space, including:

- Passwords stored in kernel memory
- Encryption keys
- Data from other processes
- Filesystem caches
- OS and driver data structures

Essentially, anything the kernel could see, user-space code could potentially be read via Meltdown.

How to prevent exploitation

A realistic solution is to separate kernel space from user space, which is called Kernel page-table isolation (KPTI), also known as KAISER. With this countermeasure, it ensures there is no valid mapping to kernel space or physical memory available in user space. Although KAISER provides basic protection against Meltdown, it has some limitations. Due to the design of the x86 architecture, several privileged memory locations are required to be mapped in user space, leaving a residual attack surface for Meltdown. But still, KAISER is the best short-time solution available and should therefore be deployed on all systems immediately.

Furthermore, besides replacing a PC's processor, the only way to close the vulnerability is to patch the operating system. For servers and cloud instances, follow your provider's security advisories and apply recommended patches/firmware. Check manufacturer's websites for the latest updates and install them right away. Although some are saying that these patches are causing systems to perform slower, it's still worth avoiding the hefty costs of noncompliance.

Conclusion

Hardware vulnerabilities specifically Meltdown present a significant risk to the security and functionality of systems. Addressing these vulnerabilities requires a comprehensive approach that includes secure design and rigorous testing. By understanding and mitigating these risks, organizations can better protect their hardware from exploitation and ensure the integrity and security of their systems.

References

Constantin, L. (2024, July 15). *39 hardware vulnerabilities: A guide to the threats*. Retrieved from CSO: https://www.csoonline.com/article/567525/hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html

Installing GitHub Desktop on Debian/Ubuntu [closed]. (n.d.). Retrieved from StackOverflow: https://stackoverflow.com/questions/73980172/installing-github-desktop-on-debian-ubuntu

isec-tugraz / meltdown. (n.d.). Retrieved from Github: https://github.com/isec-tugraz/meltdown

Meltdown - Bypass Intel's Hardware Barrier Between Applications And The Computer's Core Memory. (n.d.). Retrieved from Exploit Databse: https://www.exploit-db.com/exploits/43425

Understanding Hardware Vulnerabilities and Advanced Persistent Threats. (2024, October 2). Retrieved from Linkedin: https://www.linkedin.com/pulse/understanding-hardware-vulnerabilities-advanced-persistent-giffe#:~:text=Hardware%20vulnerabilities%20refer%20to%20weaknesses,processors%2C%20memory%2C%20and%20firmware.

What is hardware vulnerabilities? (n.d.). Retrieved from clocked-out: https://clocked-out.com/what-is-hardware-vulnerabilities/

What is Meltdown/Spectre? (n.d.). Retrieved from Cloudflare: https://www.cloudflare.com/learning/security/threats/meltdown-spectre/