Name- Mahmud, SK. Shams

ID- 13-24306-2

Advance Operating System

WHAT IS MELTDOWN & SPECTRE?

Spectre and Meltdown are the names given to a trio of variations on a vulnerability that affects nearly every computer chip. Meltdown and Spectre exploit critical vulnerabilities in modern . These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents. The Meltdown and Spectre vulnerabilities are considered "catastrophic" by security analysts.

Meltdown is a hardware vulnerability affecting Intel x86 microprocessors,IMB POWER processors and some ARM-based microprocessors. Meltdown was issued a Common Vulnerablities and Exposures ID of CVE-2017-5754, also known as Rouge Data Cache Load. Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system. Meltdown was independently discovered and reported by three teams:

Jann Horn

Warner Hass, Thomas Prescher

Daniel Gruss, Moritz Lipp, Stefan Mangard, Michel Schsarz

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre.

Spectre was independently discovered and reported by two people:

Jann Horn

Paul Kocher

Why are Spectre and Meltdown dangerous?

Spectre and Meltdown both open up possibilities for dangerous attacks. For instance, JavaScript code on a website could use Spectre to trick a web browser into revealing user and password information. Attackers could exploit Meltdown to view data owned by other users and even other virtual servers hosted on the same hardware, which is potentially disastrous for cloud computing hosts.

But beyond the potential specific attacks themselves lies the fact that the flaws are fundamental to the hardware platforms running beneath the software we use every day. Even code that is formally secure as written turns out to be vulnerable, because the assumptions underlying the security processes built into the code — indeed, built into all of computer programming — have turned out to be false.

System affected by Meltdown:

Desktop, Laptop, and Cloud computers may be affected by Meltdown. More technically, every Intel processor which implements out-of-order execution is potentially affected, which is effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013). We successfully tested Meltdown on Intel processor generations released as early as 2011. Currently, we have only verified Meltdown on Intel processors. At the moment, it is unclear whether AMD processors are also affected by Meltdown.

System affected by Spectre:

Almost every system is affected by Spectre: Desktops, Laptops, Cloud Servers, as well as Smartphones. More specifically, all modern processors capable of keeping many instructions in flight are potentially vulnerable. In particular, we have verified Spectre on Intel, AMD, and ARM processors.

Ways to Prevent Spectre and Meltdown :

1.Create a detailed inventory: Nearly every modern IT system will be affected to some extent. The starting point for security leaders must be to inventory all affected systems.

2. Develop and prioritize remediation efforts: The vulnerabilities are not remotely exploitable. A successful attack requires the attacker to execute code on the system. Whitelisting and application controls on all systems will reduce the risk of unknown code execution.

3. Recognize that patches are not always the right answer: Information security leaders must be prepared for scenarios in which a patch is not a solution. There will be a lack of patches for older systems. Patches might also fail because the impact on performance is not offset by the reduction in risk, such as with network and storage controllers.

4. Be diligent about hygiene: For systems that are not patched or only partially patched, multiple mitigating controls can reduce risk. “The single most important issue to address is restricting the ability to place untrusted/unknown code onto the device. By doing this, we significantly reduce the risks, because attacks require local code execution — for Spectre and Meltdown — and any future attacks,” says MacDonald.

5. Plan for the future, not the past: This is not the last we will see of these issues. The underlying exploitable implementation is still present and will remain so for years to come. Further research on this design flaw — involving speculative execution to discover new types of attacks— is expected and will likely require additional patches for hypervisors, OSs, browsers and firmware upgrades during the next several years.