name:Faria Hassan

id:16-31826-1

1.what is meltdown?

ans:Meltdown is a hardware vulnerability affecting Intel x86 microprocessors, IBM POWER processors, and some ARM-based microprocessors.

Meltdown affects a wide range of systems.Meltdown exploits a race condition, inherent in the design of many modern CPUs.

This occurs between memory access and privilege checking during instruction processing.A Meltdown attack cannot be detected if it is carried out.

2.what is spectre?

ans:Spectre is a vulnerability that affects modern microprocessors that perform branch prediction.Spectre is a vulnerability that tricks a program into accessing arbitrary locations in the program's memory space.

An attacker may read the content of accessed memory, and thus potentially obtain sensitive data.

3.How they work?

ans:Meltdown and Spectre exploit critical vulnerabilities in modern processors. 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.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

4.How to protect your computer from meltdown and spectre?

ans: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.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information.

This applies both to personal computers as well as cloud infrastructure.here are software patches against Meltdown.

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 is harder to exploit than Meltdown, but it is also harder to mitigate.

However, it is possible to prevent specific known exploits based on Spectre through software patches.

5.what architecture they used?

ans:they used intel x86 microprocessors, IBM power processors and some ARM-based microprocessors.