xtravirt

Cybersecurity Note

Spectre & Meltdown

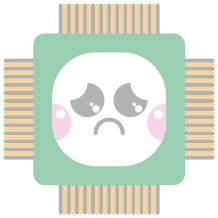
Spectre and Meltdown are hardware bugs that exploit critical vulnerabilities in modern processors. This overview has been put together by Xtravirt to assist customers in undertaking risk mitigation of this exposure.

1 What are Spectre and Meltdown?

- Both Spectre and Meltdown are vulnerabilities that have been identified in modern computing that allow programs to steal data being processed on computers using Intel, Apple, AMD and ARM processors
- **Spectre** is a **CPU architecture** vulnerability. It allows an attacker to trick programs that follow certain best practices into leaking their secrets. The usual best practice safety checks in this case actually increase the attack surface and makes applications more susceptible to Spectre. This affects all CPU vendors.
- **Meltdown** is a memory management vulnerability. It allows the attacker to bypass barriers between applications and the computers core memory. It allows a program to access the usually untouchable memory of other programs and OS (Operating System).

Spectre Bug
Exploits branch prediction & speculative execution

Meltdown Bug
Exploits Intel privilege escalation & speculative execution



Speculative Execution
CPU optimisation process that could be exploited by both bugs

2 What problems are they causing?

- Most modern computing systems now use 'best practice' technologies. It is these 'best practices' that Spectre and Meltdown exploit. This affects laptops, computers, smart phones, and by association cloud platforms.
- Currently it is not known if hackers have already exploited Spectre and Meltdown, as intrusions using Spectre and Meltdown are very hard to detect.

3 What do companies need to be doing?

- Work with Anti-Virus, Hardware and Operating System vendors to identify an update to patch the exploit permanently, including Anti-Virus engines and definition files, and then implement with minimal disruption to business services. You can view a list of vendor patches on the Xtravirt Cybersecurity web page.
- Understand and educate employees to limit the exposure to Spectre and Meltdown by identifying which systems are at risk, and how to mitigate these with minimal disruption to business services
- Identify the risk and exposure of external suppliers that provide services to the business, and their timeline to patch their systems against the exploits
- Keep on top of all the latest news on Spectre and Meltdown including, delivery methods, patches, further discoveries and any outbreaks

4 Where can organisations go for help?

- Keep an eye on the Xtravirt Cybersecurity web page for updates and guidance
- Check the Hardware and Operating System vendor websites and alerts for updates and patches

Spectre and Meltdown represent significant security vulnerabilities, but the full potential of their possible impact is still developing. Keep up to date with the latest news on xtravirt.com.