**Meltdown** and **spectre** are two different but equally harmfull,exploits in hardware. They are local, read-only exploits not known to corrupt, delete, nor modify data. For local single user laptops, such as Librem laptops, this is not as large of a threat as on shared servers—where a user on one virtual machine could access another user’s data on a separate virtual machine.

Meltdown: This vulnerability is the easiest to exploit and the one getting the most attention. It primarily affects the Intel chipset and is current being addressed with operating system level patches from Microsoft, Apple and various Linux distributions. It works by using a method called -speculative execution to infer values in protected memories

Spectre: This is a more generalized attack based on concepts similar to Meltdown and affect Arm and AMD processors in ways that the Meltdown attack can't. This also means that fixes and work arounds for Meltdown will not protect against Spectre attacks.