Flawed computer chips and how to fix them

January 5 2018

As tech giants race against the clock to fix major security flaws in microprocessors, many users are wondering what lurks behind unsettling names like "Spectre" or "Meltdown" and what can be done about this latest IT scare.

What is Meltdown? And Spectre?

These are the names given to two flaws which have been detected in most of the micro processors in use today, be it on computers, tablets, smartphones or game consoles. They are among the first flaws ever found to affect the running of every IT system in the world.

Meltdown appears for now to affect mostly chips built by US giant Intel, according to sector specialists Kaspersky Labs and Symantec.

The flaw could allow attackers to break down the barrier between user apps and the heart of the operating system, according to Kaspersky Labs, "enabling them to potentially steal data from the memory of running apps".

Anybody exploiting the flaw would get access to a complete cartography of all the files present in the device's memory at the time of the attack, by hijacking a process that was originally designed to optimize processor performance.

The Spectre threat is potentially even bigger because it concerns all chip makers: AMD and AMR as well as Intel.

What is a micro processor?

It's the central element of computers, smartphones and other digital devices, allowing them to function by carrying out instructions and handling programme data.

A processor is made up of a number of transistors. The more transistors there are, the higher the chip's capacity to handle data.

These chips are called micro-processors because processor sizes have come down significantly to integrate them into small devices. Processor power is measured in bits, a gauge of how many pieces of information a processor can handle at any one time.

What are the dangers?

Potentially they are enormous. Hackers who know what they're doing could, for example, use Meltdown to gain access to all information stored on a remote server, or cloud, so long as they rent space on the same server.

The stakes are highest for the protection of sensitive data such as passwords, pictures, personal documents and e-mails.

Cloud storage sites represent a particularly grave risk because once such a server is vulnerable, so are all data hosted there.

This is why Microsoft, Amazon or OVH have been scrambling to install updates to restore data protection on their servers.

Experts point out, however, that it takes a very high level of technical skill to exploit the Spectre and Meltdown flaws, limiting the risks

somewhat.

Michael Schwartz, an IT expert quoted in German daily Tagesspiegel Friday, said that a hacker must find out which programmes are currently running before triggering an assault, "which is why it's not that easy to launch mass attacks".

What possible protection?

For now, the only way to beef up defences is to install the security updates offered by the chip makers themselves, or by the operating systems providers: Microsoft for Windows, Apple for iOS and Google for Android and Linux.

These updates for now mostly concern Meltdown. Spectre appears, for now, to be more difficult to patch.

Either way, these updates are little more than tinkering. The safest solution would be to upgrade to a last-generation processor, a switch that will take much longer to implement because it only happens when users buy new devices.

In the meantime retail users, said Schwartz, "shouldn't panic and just behave as they would normally.

"If you follow the usual security recommendations and don't open unknown attachments or click on strange links, then you are in no immediate danger."