Bugs in modern computers leak sensitive data

The recently discovered Spectre and Meltdown vulnerabilities are said to affect the microprocessors in the majority of the world's computers, including mobile devices and cloud networks, and can allow hackers to acces the entire contents of a computer's memory.

© Leo Wolfert via 123RF

The Spectre and Meltdown vulnerabilities are bi-products of optimisation techniques designed to increase the performanc modern processors.

These techniques are called "out-of-order" and "speculative" execution. They allow the processor to make better use of tin it would have to spend waiting unnecessarily before executing the next instruction to pre-compute further results which ma or may not be used in the execution flow.

These pre-computed results, if not used, are discarded – but, as researchers have shown, there are side-effects left by su precomputation which are not disposed of thoroughly and can sometimes be leaked to the potential attacker.

As stated by the authors of the papers describing the vulnerabilities, there are theoretical ways antivirus could detect the problem. However, detection would have an extremely negative impact on the device's performance and significantly influence user experience; it would be a less effective approach than prevention.

Eset recommends that its users keep track of any related patches for their systems and apply them as soon as possible.

While Eset protects against potential malware infection, you should also take these steps to secure your computers and da

- Make sure your browser is up to date. For Chrome or Firefox users:
- Mozilla has released information describing their response, including how Firefox 57 will address these security flaws
- Google has stated, "Chrome 64, due to be released January 23, will contain mitigations to protect against exploitation In the meantime, you can enable "Site Isolation" found in current stable versions of Chrome to provide better protection.
- Make sure you update your ESET software, then update your Windows OS to protect against this exploit.
- Customers should review ESET's Knowledgebase article for important updates.
- If you have a cloud-based server or have a website hosted by hosting provider, check to see what mitigations they h implemented already to prevent Meltdown.