ESET Tech Center

Spectre and Meltdown vulnerabilities discovered

Anish | ESET Nederland - 2019-08-16 - Comments (0) - Customer Advisories

https://support.eset.com/ca6643/

Summary

ESET has recently learned about vulnerabilities called Spectre and Meltdown that affect many modern processors. ESET is one of the few third-party security solutions already compatible with Microsoft's emergency patches (released January 3rd, 2018) that fix these vulnerabilities.

Solution

On January 4, 2018, at 7:45 AM CET, ESET released Antivirus and antispyware scanner module 1533.3 for all consumer and business users. This update marks the system as compatible to download important security patches by Microsoft. At the time of writing, ESET is one of only three AV vendors to support the patches, with others set to receive the updates starting tomorrow.

Why it's important to use a Microsoft-compatible solution such as ESET

While testing the patch on Windows operating systems, Microsoft determined that some third-party applications have been making unsupported calls to Windows kernel memory. These calls have caused stop errors (also known as BSODs).

These calls may cause stop errors that make the device unable to

boot. To help prevent stop errors caused by incompatible antivirus applications, Microsoft is only offering the Windows security updates released on January 3, 2018 to devices running anti-virus software from partners who have confirmed their software is compatible with the January 2018 Windows operating system security update.

Details

The Spectre and Meltdown vulnerabilities, published on January 3, 2018, are caused by side-effects of optimization techniques designed to increase the performance of modern processors.

These techniques are called "out-of-order" and "speculative" execution. They allow the processor to make better use of time it would have to spend waiting unnecessarily before executing the next instruction to pre-compute further results which may 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 such precomputation which are not disposed of thoroughly enough 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. Therefore, we recommend that ESET users keep track of any related patches for their systems and apply them as soon as possible.

Feedback & Support

If you have feedback or questions about this issue, please contact us using the ESET Security Forum, or via local ESET Support.

Version log

Version 1.0 (January 4, 2018): Initial version of this document