Meltdown & Spectre: How to protect yourself from these CPU security flaws

2018-01-08 - Anish | ESET Nederland - Comments (0) - Security Update

January 04, 2018

By now you've likely heard about Meltdown and Spectre, the two major security flaws announced by computer experts on January 3.

According to Google's research division, Project Zero, the flaws affect the microprocessors in the majority of the world's computers, including mobile devices and cloud networks, and can allow hackers to access the entire contents of a computer's memory. You can read our in-depth article on WeLiveSecurity for more information on these flaws and a list of advisories and patch announcements released by affected vendors.

The good news is ESET was one of the very first security vendors to allow the Microsoft patch against the flaw to be enabled.

While ESET protects against potential malware infection, you should also take these steps to secure your computers and data:

- 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. To update ESET:
  - ESET Home products (NOD32 Antivirus, Internet Security, Smart Security Premium)
  - ESET Business products (Endpoint Antivirus, Endpoint Security, File and Mail Security and Virtualization Security)

- Customers should review ESET's Knowledgebase article for important

updates.
- See this great collection of tips, articles and recommendations from the Google Project Zero team.
- If you have a cloud-based server or have a website hosted by hosting provider, check to see what mitigations they have implemented already to prevent Meltdown.

Please continue to check in here periodically. We will continue to update this blog post as additional information and resources become available.

UPDATED: 10:33am PST, 5 January 2018