Best practices against the Spectre and Meltdown vulnerabilities

Anish | ESET Nederland - 2018-03-07 - Comments (0) - Customer Advisories

Issue

Best practices
News
Frequently asked questions
macOS

Solution

The Spectre and Meltdown vulnerabilities, published on January 3, 2018, are byproducts of optimization techniques designed to increase the performance of modern processors. Fixes to prevent user-mode programs from exploiting these vulnerabilities within the computer's processor are being introduced by operating system vendors. Follow the best practices in this article to secure your computers and data.

Best practices

Your ESET product protects against potential malware infection, but you should also follow the steps in Meltdown & Spectre: How to protect yourself from these CPU security flaws to secure your computers and data. You should also download the latest product modules for your ESET product.

Download the latest product modules for best protection

ESET has released an updated Antivirus and antispyware scanner (module 1533.3 in update 16680) for all consumer and business products. See the appropriate Knowledgebase article link for

instructions to update your product:

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

Note that a potential side-effect of the Microsoft patch can be reduced system speed. This is not due to the performance of your ESET product, but rather the firmware changes required to mitigate the Meltdown vulnerability within the computer's processor.

News

As of January 9th, 2018, Microsoft, Linux and Apple have released patches in response to these issues. ESET products are some of the first to offer full compatibility with Microsoft emergency patches that help protect against these issues.

We strongly encourage you to download the latest ESET product updates to allow the installation of these patches.

Keeping your ESET product updated is the best way to stay safe from threats that may take advantage of Spectre or Meltdown vulnerabilities. More information about these vulnerabilities is available in the following ESET publications:

- ESET Customer Advisory 6443: Spectre and Meltdown vulnerabilities discovered
- ESET Corporate blog post: Meltdown & Spectre: How to protect yourself from these CPU security flaws
- WeLiveSecurity blog posts
  - Meltdown and Spectre CPU Vulnerabilities: What You Need to Know
  - MADIoT – The nightmare after XMAS (and Meltdown, and Spectre)

Frequently asked Questions about Spectre and

Meltdown

Meltdown

Is ESET compatible with the Microsoft patch that corrects the Meltdown Intel Flaw?

Yes, ESET released “Antivirus and Antispyware Module 1533.3” on Wednesday, January 3rd at about 11PM Pacific Time.

Which operating systems are affected by Meltdown?

Any computer using Intel processors made between 1995 and current day are potentially affected.

Which operating systems have been patched to address the Meltdown exploit?

At this time, Apple, Linux and Microsoft have released patches. Microsoft released a Windows 10 patch available for download on January 3rd, 2018. Apple macOS, OS X iOS as well as Windows 7 and 8 patches were made available on Tuesday, January 9th, 2018.

ESET products have already been made compatible with these patches through regular product module updates. You should also be aware of patches for the Firefox, Internet Explorer and Edge web browsers that are currently available through automatic updates from their respective manufacturers. Per latest information at the time of writing, a patch for Google Chrome will be released on January 23rd. Also, you should keep a watch on your computer manufacturer’s site for any firmware updates to address the Meltdown exploit.

Spectre

Which operating systems are affected by Spectre?

Any computer using an Intel, AMD, or ARM processor is potentially affected.

How do I protect myself from Spectre?

Follow your computer/phone manufacturer for updated firmware releases.

macOS 10.13.2 and earlier

Following the installation of Apple patches for the Spectre/Meltdown vulnerabilites in the macOS versions 10.11.6 and 10.12.6 supplemental update, system errors can occur when ESET Cyber Security aor Cyber Security Pro are opened.

Click for instructions to assure compatibility of your ESET Cyber Security product and macOS