How to Protect Against Meltdown & Spectre Security Flaws

Two major security flaws have been found in modern computer processors, potentially impacting nearly all modern computers in the world.

All Macs and iOS devices along with most Windows PC and Android devices are potentially susceptible to the critical security flaws, named Meltdown and Spectre.

Theoretically, the vulnerabilities could be used to gain unauthorized access to data, passwords, files, and other personal information on any impacted computer or device.

What are Meltdown and Spectre?

The vulnerabilities are described by security researchers as follows:

> "Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware bugs allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.
>
> Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers."

Having security flaws that potentially impact nearly every computer and smart phone on the planet is obviously fairly major news, and you can read more about it here, here, or here if you're interested.

Apple has acknowledged the problem with an Apple Support article here, which cautions the following:

> "All Mac systems and iOS devices are affected, but there are no known exploits impacting customers at this time. Since exploiting many of these issues requires a malicious app to be loaded on your Mac or iOS device, we recommend downloading software only from trusted sources such as the App Store."

So what should you do? And how should you defend or protect against these security vulnerabilities?

How to Defend Against Meltdown and Spectre

The easiest way to avoid potential security trouble with Meltdown or Spectre vulnerabilities is to take a multi-prong approach to computer and device security:

- Avoid untrusted software, and never download anything from untrusted sources
- Use an updated web browser that contains relevant patches for these security flaws
- Install relevant security updates and/or system software updates when they become available for your device or computer

By the way, those are good general computer security tips to practice… even after the threat of Meltdown and Spectre passes thanks to software updates. Let's detail a bit further:

1: Avoid Sketchy Websites and Dubious Downloads

Do not download untrusted software or anything from an untrusted source, ever. Not downloading sketchy software from sketchy sources is good computing advice in general, not only to protect against Meltdown and Spectre, but also to prevent other potential malware and junkware from ending up on your computer.

Never accept an unsolicited download. Never install software that you did not specifically seek out to install. Always download and get software from trusted websites and sources, whether it's the software developer, the vendor, or a place like the App Store.

2: Update Your Web Browsers

Another potential attack vector comes from web browsers. Fortunately, major web browsers have been (or will be) updated to ward off potential problems:

- Firefox version 57 and later are apparently patched
- Google Chrome will apparently be patched on January 24 with version 64 or later
- Safari will apparently be patched in the near future for Mac, iPhone, and iPad

For Windows users, Microsoft Windows 10 and the Edge browser have been patched, and updates for other versions of Windows are due out as well. Tthe latest versions of Android have apparently been patched by Google as well.

If you're concerned about using an un-patched web browser in the meantime, you could shift to a patched browser for the interim period until the primary browser gets repaired. For example, you could download and use Firefox 57 (or later) for a few days until Safari or Chrome gets updated.

3: Install Security Updates and/or Software Updates When Available

You will want to be sure to install relevant security updates when they become available for your devices and computers.

Another option is to update operating system software to major new release versions. Apple says they have already released mitigations for Mac, iPhone, iPad, iPod touch, and Apple TV running the following system software or newer:

- iOS 11.2 or later for iPhone, iPad, iPod touch
- macOS 10.13.2 High Sierra or later for Macs
- tvOS 11.2 or later for Apple TV

It remains to be seen if Apple will issue independent security update patches for prior versions of Mac OS system software, but in the past Apple has often done this with the prior two system software releases. Hopefully macOS Sierra 10.12.6 and Mac OS X El Capitan 10.11.6 will receive separate future security software updates to protect against Meltdown and Spectre, since not all Mac users can or want to update to macOS High Sierra.

Apple Watch and watchOS are apparently not impacted.

TLDR: Significant security vulnerabilities have been discovered on basically all modern computers. Keep

an eye on the Software Update mechanism of your Mac, iPhone, iPad, other computers and smartphones, update your apps and web browsers, and install security updates when they become available.