A n ominous start to the new year.

Meltdown and Spectre

*By **Mark Costlow**, president*

The new year has brought with it two new words that all computer users will be hearing a lot. "**Meltdown**" and "**Spectre**" are the names given to two new security attacks that exploit features buried in the hearts of most computer hardware. Unlike most exploits, these do not threaten specific operating systems like Windows or MacOS, or applications like Outlook or Word or Firefox. Rather, these attacks threaten almost any software running on any operating system on any computer type (including phones and tablets).

Meltdown

The good news (if there is any) is that Meltdown, while easier for bad guys to utilize, is also easier to patch. It has to be fixed in the OS, not individual applications, so your next Windows or Linux update will contain the fixes. MacOS's current version already contains the fixes.

The downside of the Meltdown fix is that it introduces a performance penalty for "certain workloads". Without going into too much technical detail, the kind of computing that will be most impacted is that which does a lot of input/output of data. Gamers, spreadsheet cowboys, online shoppers, and power emailers will be largely unaffected. IT admins who run web-, email-, database-, and file-servers will have to consider the impacts of the fixes and whether to apply them in every case. In some situations additional computing resources will have to be added to handle the same workloads as before.

Currently, anti-virus software is throwing a wrinkle into this update on Windows servers. Most 3rd-party anti-virus software is incompatible with the Meltdown fix, so on Windows servers the fix will not be enabled if 3rd-party A/V is installed, until that A/V is updated and sets a specific registry key to show that it is ready.

Most of the large cloud providers are frantically updating the servers that customers' virtual machines run on. Some customers will also need to update their own software which runs in those clouds as well, and some won't. When in doubt, update. But, check with your cloud provider first because if you update before the patches are fully ready, you may need to update again later.

The Meltdown bug primarily only affects Intel chips and a couple of specific models of other companies' chips. Notably, Intel's only significant CPU competitor, AMD, is immune to this particular problem.

Spectre

The Spectre bug is is much harder to fix, and will require changes to all levels of software and hardware to completely eradicate. Thankfully, it is also more difficult to exploit the Spectre bug, so the urgency to fix it is not as intense. The need to fix is great, but the timeline will be weeks and months, rather than days.

The most vulnerable environment is the web browser. Proofs of concept exist for malicious

code delivered by a web page that can use the Spectre techniques to pilfer private data from other parts of the web browser, such as saved passwords and credit card numbers. Spectre-related fixes will be rolling out for OSes and application software for months to come.

What should we do to protect ourselves from these new threats? The best advice is to apply the software updates available for your devices and application software as they become available. Especially check that your Chrome, Firefox, Edge, and Safari are up-to-date.

At SWCP, we are working with our software vendors to apply patches and upgrades to our systems as quickly as possible. We strive to make these updates with as little impact to customer services as we can manage. We look forward to many late-night reboots in our near future.

The Dangers of Monoculture

An interesting aspect to the Meltdown bug is that it primarily only affects Intel chips. The fix is "easy" to make, but incurs significant performance degradation for certain server workloads. This leads one to wonder about the dangers of monoculture.

In biology, monocultures are vulnerable to being completely wiped out by a single disease or event. Biodiversity makes an ecology much more resilient to these challenges.

It is estimated that Intel owns over 90% of the datacenter CPU market. This event, which affects essentially all Intel CPUs made in at least the past decade, should serve as a wake-up call. If a single "disease" such as this bug can impact humanity's **entire electronic infrastructure**, imagine the fallout if another hardware bug is found which can't be quickly fixed in software.

Also, there are computers that will never get updates to fix this bug, and they will remain vulnerable, humming away inside society's infrastructure awaiting exploit.

Resources

The web site for your vendor is the best place to check for updates for your computer, phone, tablet, or software.

In the tech press, **Ars Technica** (**https://arstechnica.com**) has accurate "big-picture" reporting

about the various impacts of these bugs. **The Register** (**https://www.theregister.co.uk**) has also done great reporting on this issue.

Bookmark the post at our website, at **http://www.swcp.com/meltdown-and-spectre/** for the latest developments.

WordCamp 2018 Albuquerque

At SWCP, we're wild about WordPress, the most popular publishing platform on the planet, both easy to use and yet remarkably sophisticated. Therefore we are pleased to help sponsor the return of WordCamp Albuquerque this month.

WordCamp is a WordPress conference with great content geared toward all levels of WordPress users, from first-time blog owners to theme or plugin developers.

The next WordCamp Albuquerque is January 19-21 and has an amazing line-up of speakers. John Maeda, Ashleigh Axios, Chris Lema, and Sakin Shrestha are some of the top name speakers.

There are two full days of events planned. The Friday track is all about fundamentals: driving traffic to your site, Google analytics, building an e-commerce platform, security and setting up a membership site. Saturday is even fuller with three separate tracks with sessions for Business, Design, and also a technical one for Developers.

The site is at CNM Work Force Training Center, 5600 Eagle Rock Ave NE, Albuquerque, NM, just past where I-25 meets Alameda.

Check out the website at **http://2018.albuquerque.wordcamp.org** for the full schedule, information about speakers, and more. Tickets are only $20 for one day, or $30 for 2 days including a catered lunch (an absolute steal for a high-quality tech conference).