Subscribe To Data Privacy Law

Email Address *

SUBSCRIBE!

Search Posts

Categories

- Webinars & Podcasts
- Jaffe Updates
- News
- Electronic Payments Law +
- Michigan Green Law +
- Data Privacy Law +
- Immigration Law +

Download PDF

JANUARY 8, 2018 | HAILEY KIMBALL

The Intel Chip Weakness Should be a Red Flag for Your Business

If your business has not considered liability insurance for data breaches before now, now is the time. From small mom and pop shops to publicly traded entities, nearly all businesses are electronically storing some type of confidential information—be it employees' social security numbers and dates of birth or customers' credit card numbers. And while you might think you are safe, the latest potential computer hack proves that almost no one is.

Last week, researchers discovered two hardware design flaws in virtually every computer chip in the world, which could allow hackers to access sensitive data like passwords. "Meltdown" and "Spectre," as they have been dubbed by the security community, are separate, but similar, vulnerabilities. Meltdown, according to researchers "basically melts security boundaries which are normally enforced by the hardware." While Spectre "breaks the isolation between different applications" allowing "an attacker to trick error-free programs, which follow best practices, into leaking their secrets."

Both are the result of design flaws in processors. Meltdown only affects Intel, while Spectre affects Intel, AMD, and ARM.

Google has published two PDFs, which provide the technical details of Meltdown and Spectre, and are available here: https://meltdownattack.com/

The good news: The major software companies are aware of and have released or are in the process of releasing patches to fix the flaw.

Microsoft released a patch last week, which is installed automatically through an update. However, some antivirus software is incompatible and could cause stop errors (also known as the "blue screen of death"), so Microsoft has only issued the patches to users running compatible antivirus software. Microsoft advises those users who have not received the patch to contact their antivirus software vendor. A security researcher, Kevin Beaumont, has created a public spreadsheet tracking which antivirus vendors are compatible with the Microsoft patch.

More information from Microsoft can be found here: https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892/

Apple states that it "has already released mitigations in iOS 11.2, macOS 10.13.2, and tvOS 11.2 to help defend against Meltdown." The Apple Watch is unaffected by either Meltdown or Spectre. Apple plans to release mitigations in Safari to help defend against Spectre in the coming days.

More information from Apple can be found here: https://support.apple.com/en-us/HT208394

Linux has also released a patch. Find out more about it here: https://lwn.net/Articles/738975/

The bad news: experts say the patches could slow computer performance by up to 30%. Some businesses, including big banks, are slowly introducing the patch to test performance issues. Cloud providers, like Amazon and Google, have reportedly applied patches and are attempting to manage the associated performance issues. Intel says most users should not experience significant slow-down.

The really bad news: in the meantime, because this flaw is now public knowledge, hackers could be exploiting it and gaining access to confidential information, and users have no way of knowing if their systems have been compromised because, according to Google, Meltdown and Spectre are untraceable in traditional Log files. Intel and Google had planned on waiting until patches were available for all systems before disclosing the flaw. That is consistent with industry practice: generally, tech companies withhold details about security problems until there is a fix so that

hackers won't know about the weakness. Here, *The Register* reported the flaw before patches were available, forcing Intel to disclose.

While no actual hacks have been reported yet, this serves as an important reminder that every business that stores confidential information electronically (nearly all businesses) should be prepared for a data breach, no matter how secure it thinks its information is. How can you be prepared? Consider insuring your business for data breaches and talk to an expert, like the ones at Jaffe Raitt Heuer & Weiss, P.C., about steps you can take to protect your data and to prepare for the worst-case scenario. In the meantime, be sure to install your recommended software and security updates.