RobbLAW
IT Security &
Compliance Consulting

Spectre & Meltdown CPU Vulnerability Announced

What is the vulnerability and how do you protect your organization?

By: Aaron Blanco
Date: January 5, 2018

On Wednesday, January 3, 2018, the Google Project Zero team published a vulnerability in the CPU architecture of all AMD, ARM, and Intel CPU's that allows an attacker to perform a side-channel attack, which means an attacker could extract data from the CPU and do things like read encryption keys in plain text, bypass other memory protection techniques, and, at worst, leverage this vulnerability along with others to break sandbox protections.

The implications of this type of attack are very serious and the only 100% way to eliminate it is to replace all CPU's within the environment with ones that are not vulnerable. Even with the seriousness of this vulnerability, replacing all CPU's is not a viable solution so all Information Security researchers and experts recommend the following actions to mitigate the attack (in order):

1. **Implement ad-blocking software on all browsers**. This would minimize the channels in which a malicious attacker could use.
2. **Implement java-script control on browsers**. This would also minimize the channels in which an attacker could use.
3. **Test and deploy the relevant software patches that are dependent on the method in which the CPU utilizes this vulnerability**. This update must be thoroughly tested and properly vetted as current benchmarks show some organizations have reported anywhere between a 5% to 30% decrease in performance. This decrease will depend on how each individual application handles memory allocation.
4. **Utilize a continual hardware refresh cycle**. Since the only complete method of protecting against this vulnerability is to replace all CPU's, having a steady hardware refresh cycle ensures the complete removal of this vulnerability over time. It is important to validate that new hardware purchases do not contain CPU's that are still vulnerable to this attack.

To clarify, all browsers includes Chrome, Firefox, Internet Explorer, and Safari.

Taking these recommended actions will not only help mitigate this vulnerability but also assist in securing the overall environment from other potential attacks. Microsoft, Apple, and the Linux foundation have already announced they have patches available:

- **Microsoft** – Patch available in the January 3, 2018 Security Release
- **Apple** – Patch available in macOS 10.13.2, iOS 11.2 and tvOS 11.2
- **Linux** – Patch available in Linux Kernel 4.15

It has now been confirmed that this vulnerability is being exploited in the wild. As always, Robb**LAW** will be here to assist in remediating this issue and will keep you up-to-date with all relevant information as time progresses.