American Technology Services

# 2018-01 ATS Security Advisory

## CPU Vulnerabilities “Meltdown” and “Spectre”

## Summary

A new class of vulnerability was recently discovered and reported by security researchers. Two specific examples of this vulnerability, called “Meltdown” and “Spectre” can allow an attacker to read any memory content on a computer. This memory may contain information intended to be kept secret, such as passwords and other sensitive data. In cloud environments, where computing resources are shared, this vulnerability can allow an attacker to read memory on systems that belong to other tenants. Since this vulnerability affects physical hardware, it cannot be patched directly; it must be mitigated through software. Microsoft, Apple, and the Linux kernel developers have released patches to mitigate this class of vulnerability in Windows, MacOS and Linux, respectively. The available exploits for this vulnerability are only consistently successful against Intel processors.

ATS is currently working to mitigate this vulnerability in all managed systems. Customers hosted in the Azure Cloud are already protected. Operating system vendor patches are being reviewed and deployed to other managed systems.

## Details

Modern computer systems isolate memory between various user processes and kernel (operating system) processes. This is an important security feature that prevents a process from reading or writing arbitrary information from other processes or from the operating system itself. For example, a photo editing application should not be allowed to read the system memory where a password manager application stores secret passwords. Or a web server service should not be allowed to read login credentials from kernel (operating system) memory. This feature, implemented by operating systems and supported by specific processor features, strengthens the security of computer systems.

Modern processors use many clever techniques to improve performance. One technique, known as “out-of-order execution” allows a processor to look ahead and process instructions that would be delayed if processed linearly. For instance, while a process is waiting for data to be read from a hard drive, it will look ahead and process instructions that are not dependent on that data. Another technique, known as “branch prediction” allows the processor to guess which path a process will take, and then compute the instructions in the guessed path. If the guessed path is wrong, then those instructions are rolled-back with no harm to the integrity of the process.

Researchers were able to use the branch prediction and out-of-order execution techniques, along with a known side-channel attack called “FLUSH+RELOAD” to allow a user process to read kernel memory. First, the attacking program requests to read information from kernel memory. The branch prediction and out-of-order execution techniques allow this information to be read. However, this information is never shared directly with the attacker program, because of memory isolation. This information *is* stored in the processor cache. This processor cache is not directly readable by the attacking process. However, the previously developed “FLUSH+RELOAD” attack allows the attacker process to indirectly deduce the contents of the cache, allowing the attacking process to read kernel memory.

## Risk Mitigation Steps Taken by ATS on Behalf of Customers

All major operating system vendors have released patches to mitigate this vulnerability. Our clients hosted in the Microsoft Azure Cloud were already patched on 1/3/2018, and are protected from this vulnerability. All managed servers will be patched this weekend, 1/6 - 1/8. Managed workstations began receiving the patch on 1/3.

## What Can You Do?

This is a serious issue that affects almost all servers, workstations and laptops. Some tablets and phones may be affected, as well. ATS will work to mitigate these vulnerabilities to all affected managed systems. It is important that all systems are updated, including unmanaged and personal devices. Please apply patches to any unmanaged and personal computers.

Feel free to contact security@networkats.com with any questions or concerns. As always, we value hearing from our clients about general and specific security concerns so that we can provide the best possible services.