Report on Recently Publicized Widespread Processor Vulnerabilities
Date: 01/05/2018

Healthcare Cybersecurity and Communications Integration Center (HCCIC)
HHSHCCIC@HHS.GOV

SUMMARY:

A widespread vulnerability in most computer processors sold over the previous decade has been identified that could pose a threat to the protection of Healthcare and Public Health (HPH) sector sensitive data, Protected Health Information (PHI), and Personally Identifiable Information (PII). The significance of this vulnerability for the Healthcare and Public Health Sector is considered medium due to the fact that local access to the computing device is generally required, and vendors are quickly releasing appropriate software patches to mitigate the hardware vulnerability. The patches do have potential to slow down processor performance in limited cases, and organizations should exercise caution and test patches carefully before implementing on high-value assets including systems which handle PHI, PII, or are directly involved in patient treatment or imaging.

DISCUSSION:

Several security research teams recently announced a vulnerability in most computer processor chips sold for at least the previous 10 years. This vulnerability set, referred to as the Spectre and Meltdown vulnerabilities in the computer security industry, allows a malicious computer program to bypass data access restrictions and gain unauthorized access to potentially sensitive information from other programs. Such sensitive information could include items such as passwords, social security numbers, medical information, or other sensitive data. An attacker using this vulnerability would generally need local access to the computer, although there are mixed views on whether the exploit can be leveraged through compromised websites. This security flaw is present in nearly all processors produced in the last 10 years, and affects computers running Windows, Mac, Linux, and other operating systems.[i,ii,iii]

As of January 4th, 2018, many operating system vendors have released or will soon release software patches to mitigate this vulnerability. Apple reportedly addressed this flaw in its update 10.13.2 issued 17 December 2017, and Microsoft released a patch on 3 January 2018. Other software vendors have also, or will soon, issue appropriate patches. HPH sector organizations should exercise caution and test patches carefully before implementation as there have been some reported conflicts with anti-virus software packages, and there is a risk that the patches could decrease system performance by 5-30 percent in high-demand computing applications. Patches should be carefully vetted and tested accordingly before implementation on high-value assets or business-critical systems.

With regards to cloud-based computing services, Amazon AWS and Microsoft Azure cloud-hosting solutions have reportedly updated their systems to mitigate the risk of inadvertent information disclosure.[iv]

Healthcare Cybersecurity and Communications Integration Center (HCCIC)
HHSHCCIC@HHS.GOV

The significance of this vulnerability for the Healthcare and Public Health Sector is considered medium due to the fact that local access to the computing device is generally required, and vendors are quickly releasing appropriate software patches to mitigate the hardware vulnerability. These vulnerabilities are being tracked by the following CVE numbers: CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754. The US Department of Homeland Security is tracking the issue via their US-CERT website as Technical Alert TA18-004A.[v]

MITIGATION TACTICS:

HHS recommends that Healthcare and Public Health entities consider installing operating system patches to Mac, Linux, and Microsoft systems in order to mitigate the risks of this widespread processor vulnerability. Organizations should exercise appropriate caution and test patches carefully before implementation on high-value assets including systems which handle PHI, PII, and should contact device vendors before deploying patches to medical technologies that are directly involved in patient treatment and/or clinical imaging due to the potential for software conflicts or performance impacts. These patches should be applied as soon as business use-cases allow.

This report was prepared by the Healthcare Cybersecurity and Communications Integration Center (HCCIC) and coordinated with the HHS Computer Security Incident Response Center (CSIRC). This is a preliminary analysis of potential vulnerabilities that continue to be researched and analyzed. It is based on the latest available information as of the date at the top of the report. Readers are advised to search for the latest authoritative information and exercise professional judgment before taking actions related to these potential vulnerabilities.

References

[i] RedHat, "Kernel Side-Channel Attacks - CVE-2017-5754 CVE-2017-5753 CVE-2017-5715," January 3, 2017 accessed January 4, 2017; https://access.redhat.com/security/vulnerabilities/speculativeexecution; https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/
[ii] Microsoft Security Tech Center, "Security Update Guide" January 3 2018 accessed January 4 2018; https://portal.msrc.microsoft.com/en-US/security-guidance
[iii] CERT, "Vulnerability Note VU#584653:CPU hardware vulnerable to side-channel attacks," January 3, 2018 accessed January 4, 2018; https://www.kb.cert.org/vuls/id/584653
[iv] Amazon AWS Security Bulletins, "Processor Speculative Execution Research Disclosure," January 3, 2017, accessed January 4, 2018; https://aws.amazon.com/security/security-bulletins/AWS-2018-013/; January 3, 2018, accessed January 4, 2018; https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/
[v] https://www.us-cert.gov/ncas/alerts/TA18-004A