Technical Report on Widespread Processor Vulnerabilities
HHS Severity Level 2: Medium
Date: 01/12/2018

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

SUMMARY:

This report is a technical update to the previously published "Report on Recently Publicized Widespread Processor Vulnerabilities" issued 1/5/2018 covering chip vulnerabilities named Meltdown and Spectre.[i]

Both Meltdown and Spectre are vulnerabilities in how computer chips handle data that have the potential to expose sensitive information, such as protected health information (PHI), being processed on the chip. As this information is protected from disclosure under HIPAA[1], Healthcare and Public Health (HPH) entities should employ risk management processes to address these vulnerabilities and ensure the security of medical records and other PHI.

Major concerns for the HPH sector include but are not limited to:

- Challenges identifying vulnerable medical devices and accessory medical equipment and ensuring patches are validated to prevent impacts to the intended use.
- Cloud Computing: Potential PHI or Personally Identifiable Information (PII) data leakage in shared computing environments
- Web browsers: Possible PHI/PII data leakage
- Patches: Potential for service degradation and/or interruption from patches

While the two vulnerabilities are both related to how modern computer chips process instructions, there are some differences between the two. DHS has compiled the following table comparing Spectre and Meltdown:[ii]

	Spectre	**Meltdown**
CPU mechanism for triggering	Speculative execution from branch prediction	Out-of-order execution
Affected platforms	CPUs that perform speculative execution from branch prediction	CPUs that allow memory reads in out-of-order instructions
Difficulty of successful attack	High - Requires tailoring to the software environment of the victim process	Low - Kernel memory access exploit code is mostly universal
Impact	Cross- and intra-process (including kernel) memory disclosure	Kernel memory disclosure to userspace
Software mitigations	Indirect Branch Restricted Speculation (IBRS)	Kernel page-table isolation (KPTI)
	Note: This software mitigation also requires CPU microcode updates and it only mitigates Spectre variant 2	

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

The Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) is maintaining a list of vendors and patch status as part of Technical Alert (TA18-004A).[iii] Notably, Microsoft has determined that some AMD chipsets are not compatible with the current patches and has recommended suspending patches on those AMD systems.[iv]

THREAT OVERVIEW:

Medical devices and supporting medical equipment, may not resemble computers, but may run operating systems (Windows, Linux, etc.) on processors that could be vulnerable to Meltdown and Spectre. Contact medical device manufacturers through security portals, if available, for information specific to each medical device and the manufacturer's recommendations for patching medical devices.

Microsoft has a catalog update on its website for Windows XP which is sometimes used in embedded systems, which may require a high degree of customized intervention to implement.[v]

The risks of PHI data leakage is especially acute in shared infrastructure like cloud computing instances. Large cloud hosting providers (Amazon AWS or Azure) patched for Spectre and Meltdown before the vulnerabilities were made public. Other cloud managed service providers and institutional or private cloud instances may not have known about the vulnerabilities during the information embargo period before January 3, 2018; and may not have applied patches. The risks of data leakage for medical research facilities, hospitals or other HPH entities which run private cloud instances, are specifically discussed in a recent SANS webinar dated January 4, 2018. [vi]

Processors vulnerable to Meltdown are potentially susceptible to an information disclosure vulnerability in web browsers parsing certain specially-crafted JavaScript code. The vulnerability is due to the lack of proper checks on JavaScript code, leading to an exploitable information disclosure of browser data. An attacker could exploit the vulnerability by sending a crafted HTML page embedded with malicious JavaScript code. A successful attack could lead to an information leak of sensitive browser information including cookies, credentials, passwords, or payment information a user enters into a browser. In HPH sector entities, browser data could potentially include PHI. Some web-browser vendors (Chrome,[vii] Microsoft, Mozilla[viii], Safari[ix]) have released mitigations for this possible browser data leakage vulnerability. Additionally, some security vendors have released network detection signatures for the possible JavaScript exploitation of Meltdown. See below in Detection Logic.

TECHNICAL DETAILS:

These vulnerabilities depend on the "speculative execution" performance improvement feature

implemented by modern Central Processing Units (CPUs). This speculative execution enables the CPU to attempt to predict what data and instructions it will need in the near future, and the CPU fetches them from the computer's memory ahead of time. This feature is meant to improve multitasking and performance in a system and have been utilized in computing for some time. These patches disable these multitasking and speculative execution features meaning the patches have the potential to degrade computer system performance. The complexity of modern chips makes it difficult to determine what performance impact the patches may have. This is why it may be necessary to contact software vendors and perform testing of these patches, particularly for high performance applications or those which may exert a heavy load on the processor.

Since these vulnerabilities involve unauthorized access to the memory of other processes, the data that is commonly handled by the applications on the system should be a key factor in determining the risk of these vulnerabilities. These vulnerabilities are difficult to reliably exploit and have not yet been seen in the wild as of this writing. Security vendors are implementing signatures to detect attempts to exploit these vulnerabilities as they are discovered in the wild or by security researchers. The attack surface has expanded as the Mozilla project determined that these could be exploited via JavaScript, which is a language that can be executed by modern web browsers. This implies that malicious code can be executed from a website to exploit these vulnerabilities and potentially exfiltrate sensitive data.

Spectre

The Spectre exploit relies on two distinct vulnerabilities (CVE-2017-5753 and CVE-2017-5715) to exfiltrate data. Both of these exploits rely on design flaws in speculative execution features found in Modern CPUs. The first of these enables an attacker to trick the CPU into mispredicting a branch of code of the attacker's choosing. The code is then executed with improper permissions, allowing the attacker's code to access the data extracted via the second vulnerability. When the second vulnerability is leveraged, the CPU is tricked into speculatively loading the memory allocated to another application on the system. Depending on the application, this could expose potentially sensitive information such as the cryptographic keys used to protect data or the PII, PHI or PCI information handled by an application's database.

Meltdown

The meltdown attack (CVE-2017-5754) is a hardware vulnerability that tricks the CPU into speculatively loading data that has been marked unreadable or "privileged." In combination with the Spectre attack this data can be passed further through more speculatively-executed instructions to perform side-channel exfiltration. If successfully done privileged data can be presented to the attacker such as cryptographic keys used to protect data or the PII, PHI or PCI information handled by an application's database.

MITIGATION TACTICS:

To help prevent stop errors caused by incompatible anti-virus applications, Microsoft is only offering the Windows security updates released on January 3, 2018 to devices running anti-virus software from partners who have confirmed their software is compatible with the January 2018 Windows operating system security update. If you have not been offered the security update, you may be running incompatible anti-virus software and you should follow up with your software vendor.

Windows 10, Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows 7 SP1 and Windows Server 2008 R2 SP1 Customers will not receive these security updates and will not be protected from security vulnerabilities unless their anti-virus software vendor sets the following registry key:[x]

```
Key="HKEY_LOCAL_MACHINE"
Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCo
mpat" Value="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”
```

Security Researcher Kevin Beaumont compiled a list of Anti-Virus software packages and their patch status.[xi]

DETECTION LOGIC

Cisco Talos has rules to detect attacks targeting Spectre and Meltdown which are included in its rules released on January 4, 2018 and are identified with GID 1, SIDs 45357 through 45368.[xii]

Palo Alto has issued Threat ID 30276 to address Multiple CPUs Side-Channel Information Disclosure Vulnerability. Multiple CPUs are prone to an information disclosure vulnerability while parsing certain crafted JavaScript code. The vulnerability is due to the lack of proper checks on JavaScript code, leading to an exploitable information disclosure. An attacker could exploit the vulnerability by sending a crafted HTML page embedded with malicious JavaScript code. A successful attack could lead to an information leak.

Technical Report on Widespread Processor Vulnerabilities
HHS Severity Level 2: Medium
Date: 01/12/2018

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

This report was prepared by the Healthcare Cybersecurity and Communications Integration Center (HCCIC) and the HHS Computer Security Incident Response Center (CSIRC). 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.

If you have questions, comments or suggestions, please email the HCCIC at

HHSHCCIC@hhs.gov

References

[i] HCCIC, "Report on Recently Publicized Widespread Processor Vulnerabilities," 5 January 2018, accessed 8 January 2018, https://content.govdelivery.com/attachments/USDHSCIKR/2018/01/05/file_attachments/939003/HCCIC-2018-001-Spectre-Meltdown-3.pdf

[ii] US-CERT, "Vulnerability Note VU#584653- CPU hardware vulnerable to side-channel attacks," accessed January 9, 2018, https://www.kb.cert.org/vuls/id/584653

[iiiiii] US-CERT, "Alert (TA18-004A) Meltdown and Spectre Side-Channel Vulnerability Guidance," January 4 2018, accessed January 9, 2018. https://www.us-cert.gov/ncas/alerts/TA18-004A

[iv] Microsoft Support, "Windows operating system security update block for some AMD based devices," accessed January 9, 2018, https://support.microsoft.com/en-us/help/4073707/windows-operating-system-security-update-block-for-some-amd-based-devi

[v] Microsoft Update Catalog, "Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4056615) Updated 1/5/2018 accessed 1/9/2018; https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056615; Microsoft Update Catalog, "Security Update for Windows XP Embedded SP3 for x86-based Systems (KB4056941) Updated 1/5/2018 accessed 1/9/2018; https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056941

[vi] SANS Digital Forensics and Incident Response, "Meltdown and Spectre – Understanding and mitigating the threats – SANS DFIR Webcast" January 4, 2018, accessed January 8, 2018; Timestamp 45:50-48:04 https://www.youtube.com/watch?v=8FFSQwrLsfE#t=45m50s

[vii] Chromium, "Actions required to mitigate Speculative Side-Channel Attack techniques," accessed January 9, 2018, https://www.chromium.org/Home/chromium-security/ssca

[viii] Mozilla, "Speculative execution side-channel attack ("Spectre")," January 4, 2018 accessed January 9, 2018, https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

[ix] Apple, "About the security content of Safari 11.0.2," January 8 2018 accessed January 9, 2018, https://support.apple.com/en-us/HT208403

[x] Microsoft Support, "Important: Windows security updates released January 3, 2018, and antivirus software," 3 January 2018, accessed 8 January 2018, https://support.microsoft.com/en-us/help/4072699/important-information-regarding-the-windows-security-updates-released

[xi] Kevin Beaumont, Anti-Virus Patch List, January 2018, 12:15 GMT accessed 8 January 16:35 GMT, https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?usp=sharing&sle=true

[xii] Snort, "Talos Rules 2018-01-04," January 4, 2018 accessed January 9, 2018, https://snort.org/advisories/talos-rules-2018-01-04-1-4-2018