NH-ISAC TIC

Updated 01/05/2018 10:00 AM EST

TLP WHITE

Facts:

Overview

The NH-ISAC Threat Intelligence Committee (TIC) was alerted to vulnerabilities in most processor chips that have been produced since 1995. The vulnerabilities were discovered by several security research teams and publicly announced Monday evening. Meltdown and Spectre are two techniques researchers have discovered that have the potential to exploit these processor vulnerabilities. The techniques circumvent protections to expose data which could include passwords, proprietary information, or encrypted communications, depending on the technique used. There are no examples of either exploit in the wild at this time.

Meltdown Technique (Also referred to as Meltdown Vulnerability)

- Affects Intel Processors only
- Possible to patch; many patches available to prevent the Meltdown exploit technique
- Cannot be exploited remotely
- Exploits – so far – have only been in lab tests, not in the wild

The Meltdown technique affects Intel processors, and works by breaking through the barrier that prevents applications from accessing arbitrary locations in kernel memory. Segregating and protecting memory spaces prevents applications from accidentally interfering with one another's data, or malicious software from being able to see and modify data at will. Meltdown makes this fundamental process unreliable. Threat actors need access to an enterprise network or a network connection to a specific consumer device to exploit the vulnerability with the Meltdown technique.

Spectre Technique (Also referred to as Spectre Vulnerability)

- Affects Intel, AMD, and ARM Processors
- Patches are available for most major browsers, but these would only cover browser-based Spectre exploits
- Intel expects to have Microcode/Firmware updates to cover 90% of processors from the last 5 years by the end of the week
- Exploits – so far – have only been in lab tests, not in the wild

The Spectre technique affects Intel, AMD, and ARM processors, broadening its reach to include mobile phones, embedded devices, and pretty much anything with a chip in it. It works differently from Meltdown; Spectre essentially tricks applications into accidentally disclosing information that would normally be inaccessible, safe inside their protected memory area. This

is tricky for a malicious actor to execute, but because it's based on an established practice in multiple chip architectures, it's going to be even trickier to fix as the fix must be applied at the microcode level.

Patching for Meltdown
Microsoft, Linux, and Apple patches are currently available. Reports on performance impact of patches range. The reason for the performance impact is the patches simply remove specific kernel level functionality compromising a design feature of the chip to improve performance. Therefore, the operating system patches remove this functionality eliminating the possibility of exploit while also eliminating the performance improvement in the chip. Whether or not businesses should patch at this time is a business decision that balances need for processing speed against the risk. Patches should be tested in an organization's environment prior to roll out.

There is substantial evidence that a few large cloud service providers already started the patching process given the increased vulnerability for threat actors to use kernel level code to get around client boundaries at the operating system level of the device. AWS started patching in mid-December so they have been aware of this vulnerability for at least a month.

Business Impact:

The perception of this vulnerability impact is likely to be greater than the actual impact of potential compromise. Healthcare organizations may be asked to deploy patches without understanding the actual risk and the business impact of degradation of service. The likelihood of an exploit in an enterprise environment is not likely at this time. There is a higher impact for cloud service providers that could lead to leakage of partitioned customer data (if unpatched) and may have performance implications when patched.

Corrective Actions:

1. Do analysis of IT asset inventory to determine scope of impacted devices

2. Make a list of the applications highly dependent on fast throughput that may be at risk with a performance degradation of greater than 20% to determine the potential business impact

3. Test the patches in a lab or dev environment to calculate the performance impact

4. Test the MS patch paying attention to possible low-level program (antivirus) incompatibility

5. Monitor the industry for any information on exploits of this vulnerability, expanding testing to determine full performance impact for the Intel devices if necessary

6. Prepare stakeholder communication for this vulnerability to respond to inquiries from third party stakeholders and share information with third party vendors

7. Reach out to cloud infrastructure service providers and monitor chat channels for service information relevant to this vulnerability and the performance issues

8. Monitor NHISAC.org for updates

Links and References:

https://meltdownattack.com/

https://www.renditioninfosec.com/files/Rendition_Infosec_Meltdown_and_Spectre.pdf

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/

https://forums.aws.amazon.com/thread.jspa?threadID=269858

https://www.nytimes.com/2018/01/03/business/computer-flaws.html

http://www.zdnet.com/article/windows-meltdown-spectre-patches-if-you-havent-got-them-blame-your-antivirus/

https://techcrunch.com/2018/01/03/kernel-panic-what-are-meltdown-and-spectre-the-bugs-affecting-nearly-every-computer-and-device/

https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/

https://support.apple.com/en-us/HT208394

Phoronix: VM Performance Showing Mixed Impact with Linux 4.15 KPTI Patches:
https://www.phoronix.com/scan.php?page=article&item=linux-kpti-kvm&num=1

Initial Benchmarks of the Performance Impact Resulting From Linux's x86 Security Changes:
https://www.phoronix.com/scan.php?page=article&item=linux-415-x86pti&num=1

Further Analyzing The Intel CPU "x86 PTI Issue" on More Systems:
https://www.phoronix.com/scan.php?page=article&item=linux-more-x86pti&num=1

TechSpot: Testing Windows 10 Performance Before and After the Meltdown Flaw Emergency Patch:
https://www.techspot.com/article/1554-meltdown-flaw-cpu-performance-windows/

Reddit: Discussion on Benchmarking:
https://www.reddit.com/r/Amd/comments/7o0m37/requesting_benchmarks_on_amd_processors_before/

PostgresSQL: Fix for intel hardware bug will lead to performance regressions:
https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe@alap3.anarazel.de