LAUREL BRIDGE
Orchestrating Medical Imaging Workflow

Tech Note: CPU Vulnerabilities

Spectre & Meltdown CPU Vulnerability Impact Review

[Note: Please also see the references listed at the end of this summary.]

Background

Jann Horn of Project Zero stated, “We have discovered that CPU data cache timing can be abused to efficiently leak information out of mis-speculated execution, leading to (at worst) arbitrary virtual memory read vulnerabilities across local security boundaries in various contexts.

Variants of this issue are known to affect many modern processors, including certain processors by Intel, AMD and ARM. …”

So far, there are three known variants of the vulnerability:

Spectre:
- Variant 1: bounds check bypass (CVE-2017-5753 - https://nvd.nist.gov/vuln/detail/CVE-2017-5753)
- Variant 2: branch target injection (CVE-2017-5715 - https://nvd.nist.gov/vuln/detail/CVE-2017-5715)

Meltdown:
- Variant 3: rogue data cache load (CVE-2017-5754 - https://nvd.nist.gov/vuln/detail/CVE-2017-5754)

Daniel Miessler provides a useful chart as part of his 'A Simple Explanation of the Differences Between Meltdown and Spectre':

	MELTDOWN	SPECTRE
Architecture	Intel, Apple	Intel, Apple, ARM, AMD
Entry	Must have code execution on the system	Must have code execution on the system
Method	Intel Privilege Escalation + Speculative Execution	Branch prediction + Speculative Execution
Impact	Read kernel memory from user space	Read contents of memory from other users' running programs
Action	Software patching	Software patching (more nuanced)

The Fix

According to website Tom’s Hardware on 5-Jan-2018, “The fix for Meltdown, an OS-level method of mitigation called kernel page table isolation (KPTI), has now been implemented for major operating systems, including Linux, macOS, iOS, Android, and Windows. Mitigations for Spectre, which is actually two different vulnerabilities, are currently less understood, however. Fixes, so far, have involved program-level, OS-level, and hardware-level patching, but it seems there isn’t a single solution to both of the Spectre vulnerabilities.

Meltdown has a singular fix across all operating systems because the vulnerability results from an optimization present in specific CPUs, namely Intel’s and some of ARM’s. With no way to fix the CPUs, the only way is to apply a heavy-handed approach that nullifies the optimization within the OS--KPTI. It was known that KPTI would, in theory, have a real performance cost. …”

Microsoft has published client guidance at: https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

LAUREL BRIDGE
Orchestrating Medical Imaging Workflow

Performance Impact

Below is a review of limited published performance testing data collected after patches have been applied to an affected system. (8-Jan-2018)

CPU performance impact:

Early benchmark testing of systems that have had patches applied to address the Meltdown and Spectre issues are showing CPU performance impacts in the range of 0% to 4% depending on the activity being tested. Floating point and integer computation tests suggest a possible 2% to 3% compute slow down after the patches are applied.

I/O performance impact:

More significant results may occur for I/O tasks.

For NVMe SSDs (NVMe is a communications interface/protocol developed for SSDs and is designed to take advantage of the unique properties of pipeline-rich, random access, memory-based storage), the I/O impact observed on various read performance tests was significant, but generally under 8%. The impact on write performance was more significant and varied more widely, with reported throughput reduction varying from 2% to 20% for 4K write tests and as high as a 40% reduction for 512K write tests. Results reported for the ATTO Disk Benchmark across a variety of read/write sizes indicated a performance hit of as much as 40% for both read & write tests.

For SATA SSDs, the reported performance impacts were more significant. Curiously, for a report using the CrystalDiskMark, 512K read/write performance was not significantly impacted, however reports for 4K transfers showed writes dropped by up to 27% and reads by up to 19%. Results reported for the ATTO Disk Benchmark across a variety of read/write sizes did not show degradation for read tests, however write tests showed up to a 17% performance reduction.

General performance impact:

According to a summary provided by The Verge, "Microsoft also warns that Windows Server running on any silicon, especially if the server task is I/O intensive, "*shows a more significant performance impact when you enable the mitigations to isolate untrusted code within a Windows Server instance.*" Microsoft is essentially warning server customers to make a tricky choice between security and performance. "*This is why you want to be careful to evaluate the risk of untrusted code for each Windows Server instance and balance the security versus performance tradeoff for your environment,*" says Myerson." Microsoft's blog post goes on to provide many more details related to Windows servers; these are worth review by system admins; the reference is provided below.

Conclusions

The Verge's summary comment is relevant to systems like routers that are running dedicated applications; they said, "It's unusual to see Microsoft telling IT admins not to patch server systems, but the Meltdown and Spectre issues are a very unusual occurrence. If a server is only running managed code and not open to browser attacks or other code on the system then admins might avoid the firmware updates, but that runs the obvious short-term risks and the potential for having to avoid other security firmware updates in the future."

These sorts of early tests and related guidance suggest that the performance of routing applications that involve significant amounts of I/O should be monitored. While the current test results are widely scattered, there does seem to be the potential for a negative impact on router throughput when some of the fixes/updates are applied.

If routing throughput degradation, sufficient to cause concern, is observed, then one should take steps to provide additional capacity by upgrading the host systems or by adding routers to the deployed infrastructure.

LBS is conducting performance tests for Compass routing environments. Once we have meaningful data to share, this sheet will be updated.

SQL:

Microsoft has made recommendations regarding SQL Server and it would be good to also review their information as part of any local performance analysis. See: https://support.microsoft.com/en-us/help/4073225/guidance-for-sql-server

Laurel Bridge will update and re-post this information to the LBS web site as new information becomes available.
Please contact support@laurelbridge.com if you have specific concerns regarding LBS products.

Note: Please also see the references that follow at the end of this summary.

References

TechSpot – testing data:
https://www.techspot.com/article/1556-meltdown-and-spectre-cpu-performance-windows

Daniel Meissler – general overview:
https://danielmiessler.com/blog/simple-explanation-difference-meltdown-spectre/

InfoQ – more detailed overview of the vulnerability:
https://www.infoq.com/news/2018/01/meltdown-spectre-deep-dive

Project Zero – report and technical details:
https://googleprojectzero.blogspot.co.uk/2018/01/reading-privileged-memory-with-side.html

Tom's Hardware – summary of vendor responses from the news:
http://www.tomshardware.com/news/microsoft-apple-amazon-downplay-meltdown-spectre-performance-hits,36232.html

The Verge – Microsoft's summary and guidance
https://www.theverge.com/2018/1/9/16868290/microsoft-meltdown-spectre-firmware-updates-pc-slowdown

Microsoft – Understanding the performance impact of Spectre and Meltdown mitigations on Windows Systems:
https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/

Microsoft – SQL Server impact from the patches for the vulnerability:
https://support.microsoft.com/en-us/help/4073225/guidance-for-sql-server

SQLHA – list of SQL vendor resources and responses:
http://sqlha.com/2018/01/04/no-good-terrible-processor-flaw-sql-server-deployments-nearly-everything-need-know/