Transient Execution CPU Vulnerability

Subjects: Others
Contributor: HandWiki Xu

Transient execution CPU vulnerabilities are vulnerabilities in a computer system in which a speculative execution optimization implemented in a microprocessor is exploited to leak secret data to an unauthorized party. The classic example is Spectre that gave its name to this kind of side-channel attack, but since January 2018 many different vulnerabilities have been identified.

Keywords: speculative execution ; vulnerabilities ; microprocessor

1. Overview

Modern computers are highly parallel devices, composed of components with very different performance characteristics. If an operation (such as a branch) cannot yet be performed because some earlier slow operation (such as a memory read) has not yet completed, a microprocessor may attempt to *predict* the result of the earlier operation and execute the later operation *speculatively*, acting as if the prediction was correct. The prediction may be based on recent behavior of the system. When the earlier, slower operation completes, the microprocessor determines whether prediction was correct or incorrect. If it was correct then execution proceeds uninterrupted; if it was incorrect then the microprocessor rolls back the speculatively executed operations and repeats the original instruction with the real result of the slow operation. Specifically, a *transient instruction*[1] refers to an instruction processed by error by the processor (incriminating the branch predictor in the case of Spectre) which can affect the micro-architectural state of the processor, leaving the architectural state without any trace of its execution.

In terms of the directly visible behavior of the computer it is as if the speculatively executed code "never happened". However, this speculative execution may affect the state of certain components of the microprocessor, such as the cache, and this effect may be discovered by careful monitoring of the timing of subsequent operations.

If an attacker can arrange that the speculatively executed code (which may be directly written by the attacker, or may be a suitable *gadget* that they have found in the targeted system) operates on secret data that they are unauthorized to access, and has a different effect on the cache for different values of the secret data, they may be able to discover the value of the secret data.

Starting in 2017, multiple examples of such vulnerabilities were identified, with publication starting in early 2018.

In March 2021 AMD security researchers discovered that the Predictive Store Forwarding algorithm in Zen 3 CPUs could be used by malicious applications to access data it shouldn't be accessing.[2] According to Phoronix there's little impact in disabling the feature.[3]

In June 2021, two new vulnerabilities, Speculative Code Store Bypass (SCSB, CVE-2021-0086) and Floating Point Value Injection (FPVI, CVE-2021-0089), affecting *all* modern x86-64 CPUs both from Intel and AMD were discovered.[4] In order to mitigate them software has to be rewritten and recompiled. ARM CPUs are not affected by SCSB but some certain ARM architectures are affected by FPVI.[5]

In August 2021 a vulnerability called "Transient Execution of Non-canonical Accesses" affecting certain AMD CPUs was undisclosed.[6][7][8] It requires the same mitigations as the MDS vulnerability affecting certain Intel CPUs.[9] It was assigned CVE-2020-12965. Since most x86 software software is already patched against MDS and this vulnerability has the exact same mitigations, software vendors don't have to address this vulnerability.

In October 2021 for the first time ever a vulnerability similar to Meltdown was disclosed[10][11] to be affecting all AMD CPUs however the company doesn't think any new mitigations have to be applied and the existing ones are already sufficient.[12]

2. Vulnerabilities and Mitigations Summary

Mitigation Type	Comprehensiveness	Effectiveness	Performance Impact
Hardware	**Full**	**Full**	**None…Small**
Firmware Microcode Update	**Partial**	**Partial…Full**	**None…Large**
OS/VMM	**Partial**	**Partial…Full**	**Small…Large**
Software Recompilation	**Poor**	**Partial…Full**	**Medium…Large**

Hardware mitigations require change to the CPU design and thus a new iteration of hardware, but impose close to zero performance loss. Microcode updates alter the software that the CPU runs on, requiring patches to be released and integrated into every operating system and for each CPU. OS/VMM mitigations are applied at the operating system or virtual machine level and (depending on workload) often incur quite a significant performance loss. Software recompilation requires recompiling **every** piece of software and usually incur a severe performance hit.

		Affected CPU architectures and mitigations						
		Intel[13]					**AMD**[14]	
Vulnerability Name (aliases)	**CVE**	**Ice Lake**[15]	**Cascade Lake, Comet Lake**	**Whiskey Lake, Amber Lake**	**Coffee Lake (9th gen)**[16]	**Coffee Lake (8th gen)***	**Zen 1 / Zen 1+**	**Zen 2**[17]
Spectre v1 Bounds Check Bypass	**2017-5753**	**Software Recompilation**					**Software Recompilation**[18]	
Spectre v2 Branch Target Injection	**2017-5715**	**Hardware + OS**		**Microcode + OS**			**Microcode + OS/VMM**	**Hardware + OS/VMM**
SpectreRSB[19]**/ret2spec**[20] **Return Mispredict**	**2018-15572**	**OS**[21]						
Meltdown Rogue Data Cache Load	**2017-5754**	**Not affected**						
Spectre-NG v3a	**2018-3640**	**Not affected**[22]		**Microcode**		**Microcode**	**Not affected**	
Spectre-NG v4 Speculative Store Bypass	**2018-3639**	**Hardware + OS/VMM**[22]		**Microcode + OS**			**OS/VMM**	**Hardware + OS/VMM**
L1 Terminal Fault, L1TF	**2018-3615**	**Not affected**				**Microcode**	**Not affected**	
Spectre-NG Lazy FP State Restore	**2018-3665**	**OS/VMM**[23]						
Spectre-NG v1 Bounds Check Bypass Store	**2018-3693**	**OS/VMM**[24]						
Spectre-NG v1.2 Read-only Protection Bypass (RPB)	**No CVE and has never been confirmed by Intel**						**Not affected**[14]	

References

1. Kocher, Paul; Horn, Jann; Fogh, Anders; Genkin, Daniel; Gruss, Daniel. "Spectre Attacks: Exploiting Speculative Execution". https://spectreattack.com/spectre.pdf.
2. Cutress, Dr Ian. "AMD Issues Updated Speculative Spectre Security Status: Predictive Store Forwarding". https://www.anandtech.com/show/16604/amd-issues-updated-speculative-spectre-security-status-predictive-store-forwarding.
3. "Benchmarking AMD Zen 3 With Predictive Store Forwarding Disabled - Phoronix". https://www.phoronix.com/scan.php?page=article&item=amd-zen3-psf&num=1.
4. "Rage Against the Machine Clear" (in en-US). https://www.vusec.net/projects/fpvi-scsb/.
5. "Arm Developer". "Speculative Processor Vulnerability | Frequently asked questions" (in en). https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability/frequently-asked-questions.
6. "Transient Execution of Non-canonical Accesses". https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1010.
7. Musaev, Saidgani; Fetzer, Christof (2021). "Transient Execution of Non-Canonical Accesses". https://arxiv.org/ftp/arxiv/papers/2108/2108.10771.pdf.
8. Francisco, Thomas Claburn in San. "Boffins find if you torture AMD Zen+, Zen 2 CPUs enough, they are vulnerable to Meltdown-like attack" (in en). https://www.theregister.com/2021/08/30/amd_meltdown_zen/.
9. https://developer.amd.com/wp-content/resources/90343-D_SoftwareTechniquesforManagingSpeculation_WP_9-20Update_R2.pdf

Foreshadow-OS L1 Terminal Fault (L1TF)	**2018-3620**	**Not affected**	**Microcode + OS**	
Foreshadow-VMM L1 Terminal Fault (L1TF)	**2018-3646**	**Not affected**	**Microcode + OS**	
RIDL/ZombieLoad Microarchitectural Fill Buffer Data Sampling (MFBDS)	**2018-12130**	**Not affected**	**Microcode + OS**	
RIDL Microarchitectural Load Port Data Sampling (MLPDS)	**2018-12127**	**Not affected** [1]	**Not affected**	**Microcode + OS**[25]
RIDL Microarchitectural Data Sampling Uncacheable Memory (MDSUM)	**2019-11091**	**Not affected**	**Microcode + OS**	
Fallout Microarchitectural Store Buffer Data Sampling (MSBDS)	**2018-12126**	**Microcode**[26][27]	**Not affected** [2]	**Not affected**	**Microcode + OS**	**Not affected**
Spectre SWAPGS[28][29][30]	**2019-1125**	**Same as Spectre 1**		
RIDL/ZombieLoad v2 Transactional Asynchronous Abort (TAA)[31][32][33]	**2019-11135**	**Not Affected**[34]		
RIDL/CacheOut L1D Eviction Sampling (L1DES)[35][36][37]	**2020-0549**	**Microcode + OS**		
RIDL Vector Register Sampling (VRS)[35][36]	**2020-0548**	**Not Affected**		
Load Value Injection (LVI)[38][39][40][41]	**2020-0551**	**Software recompilation**		
Take a Way[42][43]		**Not affected**		**Not fixed yet (disputed**[44]**)**[45]
CROSSTalk: Special Register Buffer Data Sampling (SRBDS)[46][47][48]	**2020-0543**	**Not affected**	**Microcode**	**Not affected**
Branchdiver[49]		**No CVE, relies on unpatched systems.**[50]		

The 8th generation Coffee Lake architecture in this table **also** applies to a wide range of previously released Intel CPUs, not limited to the architectures based on Intel Core, Pentium 4 and Intel Atom starting with Silvermont.[51][52] Various CPU microarchitectures not included above are also affected, among them are IBM Power, ARM, MIPS and others.[53][54][55][56]

3. Future

Spectre class vulnerabilities will remain unfixed because otherwise CPU designers will have to disable OoOE which will entail a massive performance loss.

Intel CPUs past Ice Lake, e.g. Rocket Lake and Tiger Lake are not affected by Fallout/MSBDS.

10. Lipp, Moritz; Gruss, Daniel; Schwarz, Michael (2021-10-19). "AMD Prefetch Attacks through Power and Time" (in en). https://publications.cispa.saarland/3507/.

11. "AMD Prefetch Attacks through Power and Time". https://publications.cispa.saarland/3507/1/amd_prefetch_sec22.pdf.

12. "Side-channels Related to the x86 PREFETCH Instruction". https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1017.

13. "Affected Processors: Transient Execution Attacks & Related Security..." (in en). https://www.intel.com/content/www/us/en/develop/topics/software-security-guidance/processors-affected-consolidated-product-cpu-model.html.

14. "AMD Product Security | AMD". 2019-08-16. https://www.amd.com/en/corporate/product-security.

15. Cutress, Dr Ian. "The Ice Lake Benchmark Preview: Inside Intel's 10nm". https://www.anandtech.com/show/14664/testing-intel-ice-lake-10nm/3.

16. online, heise. "Intel Core i9-9900K mit 8 Kernen und 5 GHz für Gamer" (in de-DE). https://www.heise.de/newsticker/meldung/Intel-Core-i9-9900K-mit-8-Kernen-und-5-GHz-fuer-Gamer-4183783.html.

17. Cutress, Ian. "AMD Zen 2 Microarchitecture Analysis: Ryzen 3000 and EPYC Rome". https://www.anandtech.com/show/14525/amd-zen-2-microarchitecture-analysis-ryzen-3000-and-epyc-rome.

18. https://developer.amd.com/wp-content/resources/90343-B_SoftwareTechniquesforManagingSpeculation_WP_7-18Update_FNL.pdf

19. "Spectre Returns! Speculation Attacks using the Return Stack Buffer". https://www.usenix.org/system/files/conference/woot18/woot18-paper-koruyeh.pdf.

20. Maisuradze, Giorgi; Rossow, Christian (2018). "ret2spec: Speculative Execution Using Return Stack Buffers". Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 2109–2122. doi:10.1145/3243734.3243761. ISBN 9781450356930. Bibcode: 2018arXiv180710364M. https://dx.doi.org/10.1145%2F3243734.3243761

21. https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fdf82a7856b32d905c39afc85e34364491e46346

22. "Engineering New Protections Into Hardware" (in en). https://www.intel.com/content/www/us/en/architecture-and-technology/engineering-new-protections-into-hardware.html.

23. "INTEL-SA-00145". https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00145.html.

24. "Bounds Check Bypass Store (BCBS) Vulnerability (INTEL-OSS-10002)". https://www.intel.com/content/www/us/en/support/articles/000029382/processors.html.

25. "Intel Deep Dive CPUID Enumeration and Architectural MSRs". https://software.intel.com/security-software-guidance/insights/deep-dive-cpuid-enumeration-and-architectural-msrs.

26. "INTEL-SA-00233" (in en). https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html.

27. danielmgmi (2020-07-15), danielmgmi/icebreak, https://github.com/danielmgmi/icebreak, retrieved 2020-07-15

28. "Bitdefender SWAPGS Attack Mitigation Solutions". https://www.bitdefender.com/business/swapgs-attack.html.

29. "Documentation/admin-guide/hw-vuln/spectre.rst - chromiumos/third_party/kernel - Git at Google". https://chromium.googlesource.com/chromiumos/third_party/kernel/+/refs/tags/v4.19.65/Documentation/admin-guide/hw-vuln/spectre.rst.

30. Winder, Davey (6 August 2019). "Microsoft Confirms New Windows CPU Attack Vulnerability, Advises All Users To Update Now". Forbes. https://www.forbes.com/sites/daveywinder/2019/08/06/microsoft-confirms-new-windows-cpu-attack-vulnerability-advises-all-users-to-update-now/. Retrieved 7 August 2019.

31. "Cyberus Technology: TSX Asynchronous Abort" (in en). https://www.cyberus-technology.de/.

32. at 18:02, Shaun Nichols in San Francisco 12 Nov 2019. "True to its name, Intel CPU flaw ZombieLoad comes shuffling back with new variant" (in en). https://www.theregister.co.uk/2019/11/12/zombieload_cpu_attack/.

33. Cimpanu, Catalin. "Intel's Cascade Lake CPUs impacted by new Zombieload v2 attack" (in en). https://www.zdnet.com/article/intels-cascade-lake-cpus-impacted-by-new-zombieload-v2-attack/.

34. "Intel Deep Dive TSX Asynchronous Abort" (in en). https://software.intel.com/security-software-guidance/insights/deep-dive-intel-transactional-synchronization-extensions-intel-tsx-asynchronous-abort.

35. "MDS Attacks: Microarchitectural Data Sampling". https://mdsattacks.com/#ridl-nng.

36. "IPAS: INTEL-SA-00329" (in en-US). 2020-01-27. https://blogs.intel.com/technology/2020/01/ipas-intel-sa-00329/.

37. "CacheOut". https://cacheoutattack.com/.
38. at 17:00, Thomas Claburn in San Francisco 10 Mar 2020. "You only LVI twice: Meltdown The Sequel strikes Intel chips – and full mitigation against data-meddling flaw will cost you 50%+ of performance" (in en). https://www.theregister.co.uk/2020/03/10/lvi_reverse_meltdown_intel_attack/.
39. "LVI: Hijacking Transient Execution with Load Value Injection". https://lviattack.eu/.
40. "INTEL-SA-00334" (in en). https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00334.html.
41. "Deep Dive: Load Value Injection". https://software.intel.com/security-software-guidance/insights/deep-dive-load-value-injection.
42. "Take A Way: Exploring the Security Implications of AMD'sCache Way Predictors". https://mlq.me/download/takeaway.pdf.
43. March 2020, Paul Alcorn 07. "New AMD Side Channel Attacks Discovered, Impacts Zen Architecture" (in en). https://www.tomshardware.com/news/new-amd-side-channel-attacks-discovered-impacts-zen-architecture.
44. Alcorn, Paul (March 9, 2020). "New AMD Side Channel Attacks Discovered, Impacts Zen Architecture (AMD Responds)". https://www.tomshardware.com/uk/news/new-amd-side-channel-attacks-discovered-impacts-zen-architecture.
45. Cimpanu, Catalin. "AMD processors from 2011 to 2019 vulnerable to two new attacks" (in en). https://www.zdnet.com/article/amd-processors-from-2011-to-2019-vulnerable-to-two-new-attacks/.
46. "CROSSTalk" (in en-US). https://www.vusec.net/projects/crosstalk/.
47. "Deep Dive: Special Register Buffer Data Sampling". https://software.intel.com/security-software-guidance/insights/deep-dive-special-register-buffer-data-sampling.
48. "INTEL-SA-00320" (in en). https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00320.html.
49. "BlindSide" (in en-US). https://www.vusec.net/projects/blindside/.
50. Francisco, Thomas Claburn in San. "Don't be BlindSided: Watch speculative memory probing bypass kernel defenses, give malware root control" (in en). https://www.theregister.com/2020/09/10/dont_be_blindsided_speculative_memory/.
51. "INTEL-SA-00088" (in en). https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00088.html.
52. "INTEL-SA-00115" (in en). https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html.
53. "Meltdown and Spectre Status Page". https://wiki.netbsd.org/security/meltdown_spectre/.
54. Ltd, Arm. "Speculative Processor Vulnerability | Cache Speculation Issues Update" (in en). https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability/latest-updates/cache-speculation-issues-update.
55. "About speculative execution vulnerabilities in ARM-based and Intel CPUs" (in en). https://support.apple.com/en-us/HT208394.
56. "Potential Impact on Processors in the POWER Family" (in en-US). 2019-05-14. https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/.

Retrieved from https://encyclopedia.pub/entry/history/show/78754