Vulnerabilities Associated with CPU Speculative Execution

Overview

Modern CPUs have speculative execution capabilities, which improves processor performance. Depending on the design and architecture of the CPU, speculative execution can introduce side-channel-attack vulnerabilities.

Known Vulnerabilities

Public	CVE	Alias (es)	CPU Vendors Affected	Speculative Trigger	Impact	Mitigations	References
Jan 3, 2018	CVE-2017-5753	Spectre V1 NetSpectre (network attack vector) Spectre-PHT	Intel ARM IBM	Branch prediction bounds check bypass	Cross- and intra-process (including kernel) memory disclosure	OS Compiler Browser	https://www.kb.cert.org/vuls/id/584653 https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/
Jan 3, 2018	CVE-2017-5715	Spectre V2 Spectre-BTB	Intel AMD ARM IBM	Branch target injection	Cross- and intra-process (including kernel) memory disclosure	Microcode	https://www.kb.cert.org/vuls/id/584653 https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html https://www.amd.com/en/corporate/security-updates https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/
Jan 3, 2018	CVE-2017-5754	Spectre V3 Meltdown Meltdown-US	Intel IBM	Out-of-order execution	Kernel memory disclosure to userspace	OS	https://www.kb.cert.org/vuls/id/584653 https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/
May 21, 2018	CVE-2018-3640	Spectre V3a (RSRE) Meltdown-GP	Intel ARM	System register read	Disclosure of system register values	Microcode	https://www.kb.cert.org/vuls/id/180049 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
May 21, 2018	CVE-2018-3639	Spectre V4 (SSB) Spectre-STL	Intel AMD ARM IBM	Memory reads before prior memory write addresses known	Cross- and intra-process (including kernel) memory disclosure	Microcode OS	https://www.kb.cert.org/vuls/id/180049 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html https://www.amd.com/en/corporate/security-updates https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/
Jun 13, 2018	CVE-2018-3665	Lazy FP Meltdown-NM	Intel	Lazy FPU state restore	Leak of FPU state	OS	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00145.html
July 10, 2018	CVE-2018-3693	Spectre1.1 Spectre-PHT	Intel	Bounds check bypass store	Speculative buffer overflow Cross- and intra-process (including kernel) memory disclosure	OS	https://01.org/security/advisories/intel-oss-10002 https://arxiv.org/abs/1807.03757

July 10, 2018	N/A	Spectre1.2 Meltdown-RW	Intel	Read-only protection bypass	Overwrite read-only data and pointers Cross- and intra-process (including kernel) memory disclosure	OS	https://01.org/security/advisories/intel-oss-10002 https://arxiv.org/abs/1807.03757
August 14, 2018	CVE-2018-3615	L1 Terminal Fault: SGX Foreshadow-SGX Meltdown-P	Intel	Transient out-of-order execution	SGX enclave memory disclosure	Microcode TCB Recovery	https://www.kb.cert.org/vuls/id/982149 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://foreshadowattack.eu/ https://foreshadowattack.eu/foreshadow.pdf
August 14, 2018	CVE-2018-3620	L1 Terminal Fault: OS/SMM Foreshadow-OS Foreshadow-NG Meltdown-P	Intel IBM	Transient out-of-order execution	OS or SMM memory disclosure	Microcode OS	https://www.kb.cert.org/vuls/id/982149 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/ https://foreshadowattack.eu/ https://foreshadowattack.eu/foreshadow-NG.pdf
August 14, 2018	CVE-2018-3646	L1 Terminal Fault: VMM Foreshadow-VMM Foreshadow-NG Meltdown-P	Intel IBM	Transient out-of-order execution	Virtual Machine Monitor (VMM) memory disclosure	Microcode OS	https://www.kb.cert.org/vuls/id/982149 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/ https://foreshadowattack.eu/ https://foreshadowattack.eu/foreshadow-NG.pdf
November 13, 2018		Spectre-PHT-CA-OP	Intel ARM AMD	Pattern History Table			https://arxiv.org/abs/1811.05441
November 13, 2018		Spectre-PHT-CA-IP	Intel ARM AMD	Pattern History Table			https://arxiv.org/abs/1811.05441
November 13, 2018		Spectre-PHT-SA-OP	Intel ARM AMD	Pattern History Table			https://arxiv.org/abs/1811.05441
November 13, 2018		Spectre-BTB-SA-IP	Intel ARM AMD	Branch Target Buffer			https://arxiv.org/abs/1811.05441
November 13, 2018		Spectre-BTB-SA-OP	Intel	Branch Target Buffer			https://arxiv.org/abs/1811.05441
November 13, 2018		Meltdown-PK	Intel	Protection Keys			https://arxiv.org/abs/1811.05441
November 13, 2018		Meltdown-BND	Intel AMD	Bound instruction			https://arxiv.org/abs/1811.05441

May 14, 2019	CVE-2019-11091	Zombieload MDSUM	Intel	Transient out-of-order execution	Cross- and intra-process (including kernel) memory disclosure	Microcode OS/Hypervisor	https://zombieloadattack.com/zombieload.pdf https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html https://software.intel.com/security-software-guidance/software-guidance/microarchitectural-data-sampling https://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-data-sampling https://support.google.com/faqs/answer/9330250 https://www.chromium.org/Home/chromium-security/mds https://aws.amazon.com/security/security-bulletins/AWS-2019-004/ https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013 https://xenbits.xen.org/xsa/advisory-297.html https://support.apple.com/en-us/HT210107 https://access.redhat.com/security/vulnerabilities/mds https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/MDS
May 14, 2019	CVE-2018-12127 CVE-2018-12130	RIDL MLPDS MFBDS	Intel	LFB and load port	Cross- and intra-process (including kernel) memory disclosure	Microcode OS/Hypervisor	https://mdsattacks.com/files/ridl.pdf https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html https://software.intel.com/security-software-guidance/software-guidance/microarchitectural-data-sampling https://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-data-sampling https://www.bitdefender.com/files/News/CaseStudies/study/257/Bitdefender-Whitepaper-YAM-en-EN.pdf https://support.google.com/faqs/answer/9330250 https://www.chromium.org/Home/chromium-security/mds https://aws.amazon.com/security/security-bulletins/AWS-2019-004/ https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013 https://xenbits.xen.org/xsa/advisory-297.html https://support.apple.com/en-us/HT210107 https://access.redhat.com/security/vulnerabilities/mds https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/MDS

May 14, 2019	CVE-2018-12126	Fallout MSBDS	Intel	Store Buffer and WTF optimization	Cross- and intra-process (including kernel) memory disclosure	Microcode OS/Hypervisor	https://mdsattacks.com/files/fallout.pdf https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html https://software.intel.com/security-software-guidance/software-guidance/microarchitectural-data-sampling https://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-data-sampling https://support.google.com/faqs/answer/9330250 https://www.chromium.org/Home/chromium-security/mds https://aws.amazon.com/security/security-bulletins/AWS-2019-004/ https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013 https://xenbits.xen.org/xsa/advisory-297.html https://support.apple.com/en-us/HT210107 https://access.redhat.com/security/vulnerabilities/mds https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/MDS
November 12, 2019	CVE-2019-11135	TAA	Intel	TSX Asynchronous Abort	Cross- and intra-process (including kernel) memory disclosure	Microcode	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00270.html https://software.intel.com/security-software-guidance/insights/deep-dive-intel-transactional-synchronization-extensions-intel-tsx-asynchronous-abort
January 27, 2020	CVE-2020-0548	VRS	Intel	Vector Register Sampling	Cross- and intra-process (including kernel) memory disclosure	Microcode	https://blogs.intel.com/technology/2020/01/ipas-intel-sa-00329/ https://software.intel.com/security-software-guidance/software-guidance/vector-register-sampling https://software.intel.com/security-software-guidance/insights/processors-affected-vector-register-sampling
January 27, 2020	CVE-2020-0549	CacheOut L1DES	Intel	L1D Eviction Sampling	Cross- and intra-process (including kernel) memory disclosure	Microcode	https://blogs.intel.com/technology/2020/01/ipas-intel-sa-00329/ https://software.intel.com/security-software-guidance/software-guidance/l1d-eviction-sampling https://software.intel.com/security-software-guidance/insights/processors-affected-l1d-eviction-sampling
March 6, 2020		L1D Collide+Probe	AMD	L1D cache way predictor µTag collisions	Cross- and intra-process (including kernel) memory disclosure	OS/Hypervisor	https://mlq.me/download/takeaway.pdf https://www.amd.com/en/corporate/product-security
March 6, 2020		L1D Load+Reload	AMD	L1D cache way predictor for aliased addresses	Cross- and intra-process (including kernel) memory disclosure	OS/Hypervisor	https://mlq.me/download/takeaway.pdf https://www.amd.com/en/corporate/product-security
March 10, 2020	CVE-2020-0551	LVI	Intel	Load Value Injection	SGX enclave memory disclosure	TCB Recovery	https://lviattack.eu/ https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00334.html
March 14, 2024		GhostRace	AMD, Intel, Linux, Xen	Race condition on a transiently executed path originating from a mis-speculated branch	Speculative Race Condition (SRC) vulnerability	Linux Kernel patch, Xen Virutalization Patch, AMD OS and Virtlaization API changes recommended.	https://kb.cert.org/vuls/id/488902 https://xenbits.xen.org/xsa/advisory-453.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7016.html
April 9, 2024	CVE-2024-2201		Intel, Linux, Xen	Researchers have discovered exploitable gadgets in the Linux kernel and that those are sufficient at bypassing deployed Intel mitigations.	Spectre v2 vulnerability that cannot be protected by eBPF	Linux Kernel patch, XenAdvisory	https://kb.cert.org/vuls/id/155143

Notes

General

The causes of these vulnerabilities are rooted in CPU hardware design choices intended to optimize performance.
https://lwn.net/Articles/755419/
https://pdfs.semanticscholar.org/2209/42809262c17b6631c0f6536c91aaf7756857.pdf

Other Information

NSA guidance on speculative execution vulnerabilities includes a similar list.
https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance

Spectre V1

Spectre V1 has been demonstrated to bypass protections provided by Intel SGX. Intel has updated the SGX SDK to mitigate these vulnerabilities when SGX enclaves are rebuilt.
https://software.intel.com/sites/default/files/managed/e1/ec/SGX_SDK_Developer_Guidance-CVE-2017-5753.pdf

Spectre V1 has been demonstrated to bypass protections provided by the System Management Range Register (SMRR) to access protected System Management Mode (SMM) memory.
https://blog.eclypsium.com/2018/05/17/system-management-mode-speculative-execution-attacks/

Spectre V1 can be exploited over network connections rather than through local code execution of remotely delivered code such as JavaScript. This remote attack is known as NetSpectre.
https://misc0110.net/web/files/netspectre.pdf

Lazy FP

Lazy FP may particularly expose AES keys:

> *The FPU state may contain sensitive information such as cryptographic keys. As an example, the Intel AES instruction set (AES-NI) uses FPU registers to store round keys. It is only possible to exploit when the underlying operating system or hypervisor uses lazy FPU switching.*
> *https://blog.cyberus-technology.de/posts/2018-06-06-intel-lazyfp-vulnerability.html*