Risk Assessment and Mitigation: Intel Corporation

| Vulnerability & Potential Threat #1 |
| --- |
| Meltdown is an exploitation “of side effects of out-of-order execution on modern processors to read arbitrary kernel-memory locations including personal data and passwords. Out-of-order execution is an indispensable performance feature and present in a wide range of modern processors. The attack works on different Intel microarchitectures since at least 2010 and potentially other processors are affected. The root cause of Meltdown is the hardware. The attack is independent of the operating system, and it does not rely on any software vulnerabilities. Meltdown breaks all security assumptions given by address space isolation as well as paravirtualized environments and, thus, every security mechanism building upon this foundation. On affected systems, Meltdown enables an adversary to read memory of other processes or virtual machines in the cloud without any permissions or privileges, affecting millions of customers and virtually every user of a personal computer. “ (Lipp, Schwarz, Gruss, Prescher, Haas, Mangard, Kocher, Genkin, Yarom, Hamburg, 2018) |
| Potential Risk |
| Leakage of sensitive client information such as usernames and passwords through an exploitation found in the X86 series of Intel microprocessors. |
| Risk Assessment |
| This attack exploits a hardware vulnerability, not software. The operating system of the CUP nor the microcode have not been found to contribute to this flaw. Since discovered in 2010, this architecture flaw has the innate ability to corrupt any system an Intel processor is used in. The corruption of any system can lead to potential data leakages since it allows a malicious user to potentially access the usernames and passwords of millions of users. |
| Mitigation  Changes in the architecture of the Xenon 8th gen core processors should help in alleviating the possibly of this breech. Older CPU’s still in use will be issued a microcode update to protect against this breach. (Coldewey, 2018) |

| Vulnerability & Potential Threat #2 |
| --- |
| Spectre involves “inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary. This paper [Spectre Attacks: Exploiting Speculative Execution] describes practical attacks that combine methodology from side channel attacks [SCA’s], fault attacks, and return-oriented programming that can read arbitrary memory from the victim's process. More broadly, the paper shows that speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, static analysis, containerization, just-in-time (JIT) compilation, and countermeasures to cache timing/side-channel attacks.” (Kocher, Genkin, Gruss, Haas, Hamberg, Lipp, Mangard, Prescher, Schwarz, Yarom, 2018)  Currently there are 3 known variations of this attack. The second variation has been patched by Intel, but variations 1 and 4 are still in progress of being addressed and patched successfully (variation 3 is known as a Meltdown attack as discussed in threat 1). Variation 4 allows a trespasser to exploit hardware responses to “language-based runtime environments” (Fingas, J. ,2018) (Javascript for example). This intern allows an attack through any web-browser programs being executed by a user. |
| Potential Risk |
| Leakage of sensitive information from a computer’s processor; namely user names and passwords. |
| Risk Assessment |
| The attack itself exploits a hardware vulnerability. This in tern can put a users information at risk. |
| Mitigation |
| Software patches have been developed to prevent variation 2 from being a risk to users. Patches are still in progress to address variation 4 and variation 1 of Spectre. Newer processors in development are being adjusted to incorporate counter measures against these breaches. |

| Vulnerability & Potential Threat #3 |
| --- |
| Portsmash being the exploitation of a process through SCA’s in microprocessors that operate using a “Simultaneous Multithreading (SMT) architecture” (Cimpanu, 2018); that in turn allowing multiple threads to execute in a CPU core). |
| Potential Risk |
| Leakage of vulnerable information assets from clientele computing systems. Any processor utilizing SMT architecture is at risk of this type of attack. |
| Risk Assessment |
| Intel® 64 and IA32 Architectures (Intel, 2017) utilize a variation of SMT technology and in turn are susceptible to attach through Portsmashing. If no countermeasures are devised this can lead to unintentional data breaches on clienteles’ devices. |
| Mitigation |
| New software analysis tools in development to offer countermeasures to SMT breeches. Redesign of next generation CPU’s incorporating SMT technology. (Intel, 2019). |

| Vulnerability & Potential Threat #4 |
| --- |
| Microcode, being the very software that instructs the transistor configurations within a CPU on how to carry out their operation and processing of data (whether by bit or threaded) being transferred into the contacts of the CPU itself. |
| Potential Risk |
| Vulnerabilities within the microcode itself could potentially lead to an outside party trespassing and potentially gaining control of the CPU as well as its connected systems. |
| Risk Assessment |
| Exploitation of microcode could potentially lead to the leakage of information assets on clientele computer systems and networks. It potentially also leads to the hijacking and possible damage and/or destruction of client’s computer systems or networks. |
| Mitigation |
| New software patches put in place to close known holes within microcode. Bug bounty program enacted to entice users to report faults to Intel directly. (Intel, 2019) |

| Vulnerability & Potential Threat #5 |
| --- |
| L1 terminal fault being a software glitch in which a processors memory address does not match its virtual address also in turn leading to a failure in the implementation of SGX [Software Guard Exceptions] protected memory checks and Extended Page Table (EPT) checks. (Intel, 2019) |
| Potential Risk |
| Failure to correct this can lead to the extraction of data from a vulnerable CPU given the lack of response for a SGX protected memory check or EPT check. |
| Risk Assessment |
| L1 terminal fault allowing a trespassing party access to a client’s information through their network’s CPUs. |
| Mitigation |
| Microcode from effected units pulled. A software patch was devised by Intel to correct this issue. “Deploying OS and VMM updates is also required to mitigate L1TF.” (Intel, 2019) |

References

* Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., Hamburg, M.,  (2018). Meltdown. Retrieved from <https://arxiv.org/abs/1801.01207>
* Coldewey, D. (2018).  Intel Announces Hardware Fixes For Spectre And Meltdown On Upcoming Chips. Retrieved from <https://techcrunch.com/2018/03/15/intel-announces-hardware-fixes-for-spectre-and-meltdown-on-upcoming-chips/>
* Kocher, P. Genkin, D., Gruss, D., Haas, W., Hamberg, M., Lipp, M. Mangard, S., Prescher, T., Schwarz, M., Yarom. Y.,  (2018). Spectre Attacks: Exploiting Speculative Execution. Retrieved from <https://arxiv.org/abs/1801.01203>
* Fingas, J. (2018). Intel Details Fourth Spectre-Style Cpu Security Flaw. Retrieved from <https://www.engadget.com/2018/05/21/intel-details-fourth-spectre-style-cpu-exploit/?ncid=txtlnkusaolp00000616>
* Cimpanu, C. (2018). Intel Cpus Impacted By New Portsmash Side-Channel Vulnerability. Retrieved from <https://www.zdnet.com/article/intel-cpus-impacted-by-new-portsmash-side-channel-vulnerability/>
* Intel. (2017). Intel® 64 And Ia32 Architectures Performance Monitoring Events. Retrieved from <https://software.intel.com/sites/default/files/managed/8b/6e/335279_performance_monitoring_events_guide.pdf?ref=hvper.com>
* Intel. (2019). Security First. Retrieved from <https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html>
* Intel. (2019). The Latest Security Information On Intel® Products.. Retrieved from <https://www.intel.com/content/www/us/en/security-center/bug-bounty-program.html>
* Intel. (2019). L1 Terminal Fault / Cve-2018-3615 , Cve-2018-3620,cve-2018-3646 / Intel-Sa-00161. Retrieved from <https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault>