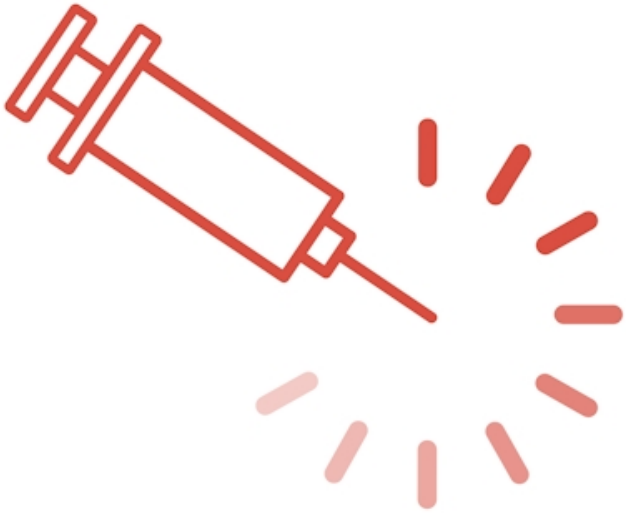
The same team of researchers behind the discovery of microarchitectural attacks such as Meltdown, Spectre and Zombieload uncover yet another exploit lurking inside Intel CPUs-- Load Value Injection (LVI), a flaw allowing "reverse Meltdown" attacks.



Discovered on 4 April 2019 and reported to Intel before public disclosure on 10 March 2020, LVI turns previous data extraction attacks and defeats all existing mitigations at both software and hardware levels. According to the researchers, this makes LVI "much harder to mitigate" compared to previous attacks, and can affect just about any access to memory. Intel was involved with the disclosure, and says it affects Atom, Core and Xeon processors, as well as the newest Ice Lake (10th Gen) chips and even the upcoming Tremont Atom core.

An LVI exploit involves four steps. First, the attacker fills a microarchitectural buffer with a value. This induces a fault or assisted load within the victim software by redirecting dataflow. The attacker's value invokes a "code gadget," allowing the running of attacker instructions. Finally, the attacker hides traces of the attack to stop detection by the processor. The process makes LVI a more direct attack compared to previous microarchitectural exploits, and so far it can defeat current Intel secure enclave architecture such as Software Guard Extensions (SGX).

That said, SGX is rarely used in SGX consumer systems outside of DRM applications. The risk is greater for enterprise and business users due to the more widespread use of SGX, not to mention shared systems. Intel and the researchers have a potential solution to LVI attacks in the shape of a code level fix with compiler and SDK updates adding a "fence," or a piece of code ensuring a program running across several cores stops at a particular point. This might hurt performance, with the impact slowing operations down from 2 to 19 times according to

researcher calculations.

Considering the above mentioned performance overheads, Intel suggests sys-admins and developers to carefully go through what needs to be patched up against LVI, especially in the case of environments where the OS and VMM are trusted.

Go Hijacking Transient Execution with Load Value Injection