computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-020

Speculative Execution Attack on Intel Processors

August 16, 2018 — v1.0

History:

- *16/08/2018 — v1.0: Initial publication*

Summary

In January 2018, two separate teams discovered flaws in Intel processor allowing speculative execution attacks and notified Intel of their researches [1]. On 14th of August 2018, the vulnerabilities were disclosed publicly under the name **Foreshadow** [2].

Based on the provided technical details Intel investigated further and identified two other attack channel with the potential to impact additional microprocessors, operating systems, system management mode, and virtualization software [3].

Intel published a security advisory providing guidance to mitigate these issues [3].

Technical Details

The three vulnerabilities received CVEs:

- CVE-2018-3615 - L1 Terminal Fault: SGX
- CVE-2018-3620 - L1 Terminal Fault: OS/SMM
- CVE-2018-3646 - L1 Terminal Fault: VMM

These three vulnerabilities may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user authorization.

L1 Terminal Fault (L1TF) happens because of a CPU optimization on page table walk. By exploiting terminal page fault exception on vulnerable CPUs, an attacker can initiate a read and forward from the L1 cache data, leading to disclosure of the data stored in the physical address referenced by the virtual address if it exist in the L1 data cache.

Products Affected

All operating systems or equipments running on the following processor may be affected by the vulnerabilities:

- Intel® CoreTM i3 processor (45nm and 32nm)
- Intel® CoreTM i5 processor (45nm and 32nm)
- Intel® CoreTM i7 processor (45nm and 32nm)
- Intel® CoreTM M processor family (45nm and 32nm)
- 2nd generation Intel® CoreTM processors
- 3rd generation Intel® CoreTM processors
- 4th generation Intel® CoreTM processors
- 5th generation Intel® CoreTM processors
- 6th generation Intel® CoreTM processors
- 7th generation Intel® CoreTM processors
- 8th generation Intel® CoreTM processors
- Intel® CoreTM X-series Processor Family for Intel® X99 platforms
- Intel® CoreTM X-series Processor Family for Intel® X299 platforms
- Intel® Xeon® processor 3400 series
- Intel® Xeon® processor 3600 series
- Intel® Xeon® processor 5500 series
- Intel® Xeon® processor 5600 series
- Intel® Xeon® processor 6500 series
- Intel® Xeon® processor 7500 series
- Intel® Xeon® Processor E3 Family
- Intel® Xeon® Processor E3 v2 Family
- Intel® Xeon® Processor E3 v3 Family
- Intel® Xeon® Processor E3 v4 Family
- Intel® Xeon® Processor E3 v5 Family
- Intel® Xeon® Processor E3 v6 Family
- Intel® Xeon® Processor E5 Family
- Intel® Xeon® Processor E5 v2 Family
- Intel® Xeon® Processor E5 v3 Family
- Intel® Xeon® Processor E5 v4 Family
- Intel® Xeon® Processor E7 Family
- Intel® Xeon® Processor E7 v2 Family
- Intel® Xeon® Processor E7 v3 Family
- Intel® Xeon® Processor E7 v4 Family
- Intel® Xeon® Processor Scalable Family
- Intel® Xeon® Processor D (1500, 2100)

Recommendations

Check your Operating System provider for update mitigating these vulnerabilities. For Windows systems, Microsoft published an advisory detailing affected versions [4].

References

[1] https://foreshadowattack.eu/

[2] https://www.youtube.com/watch?v=ynB1inl4G3c

[3] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html

[4] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv180018