CERT-EU Security Advisory 2018-001

Meltdown and *Spectre* Critical Vulnerabilities

January 11, 2018 — v1.1

History:

- *08/01/2018 — v1.0: Initial publication*
- *11/01/2018 — v1.1: Some corrections and additional sources added*

Summary

Design flaws in modern computer processors allow programs to steal data processed on the computer. The hardware design deficiencies leaded to the development of two attack scenarios:

Meltdown – *melts* security boundaries normally enforced by the processors hardware.

Spectre – *speculative execution* which leads to information disclosure.

Meltdown and Spectre vulnerabilities affect personal computers, mobile devices, and cloud services.

Operating systems and applications vendors started issuing patches to protect from the chip-level security bug. The coordinated disclosure of the details has been planned for 9th of January, but many details have become known in advance.

Technical Details

Programs typically are not permitted to read data from other programs. A malicious program can exploit Meltdown and Spectre to read in the memory space of other running programs. This might include sensitive data.

Meltdown exploits side effects of *out-of-order execution* on modern processors to read arbitrary kernel memory locations. Out-of-order execution is an performance feature present in a wide range of modern processors. 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 para-virtualized environments, and thus every security mechanism building upon this foundation. It affects most Intel and some ARM processors. AMD processors are likely not affected [1].

Spectre attacks involve inducing a victim to *speculatively execute* operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary. It affects Intel, AMD, and ARM processors [2].

The vulnerabilities received several CVEs [3]:

Spectre:

- CVE-2017-5753 (bounds check bypass)
- CVE-2017-5715 (branch target injection)

Meltdown:

- CVE-2017-5754 (rogue data cache load)

Products Affected

Meltdown affects Intel microarchitectures since 2010 and potentially other CPUs of other vendors [1]. Unlike Meltdown, the Spectre attack works also on non-Intel processors, including AMD and ARM processors [2].

- A exhaustive list of Intel affected products can be found in [4].
- For ARM processors, impact can be verified in [5].
- Unfortunately, AMD did not provide many details at this time [6, 7].

Recommendations

For Microsoft products, in order to check if vulnerable, use PowerShell verification as described here [15]. For Linux there is an open source script [19]. Please review and test before running on production systems.

Until patch for microcode of the processors or other solutions became available, the only option is to update the operating systems and applications as soon as possible. At the moment of writing, this should mitigate some issues (Meltdown), but not others (Spectre).

Below are references for various vendor-specific advisories:

- Redhat [9]
- Suse [10]
- Microsoft [11]
- Google/Android [12]
- Mozilla [13]
- Amazon [14]
- Apple [20]

A note for Microsoft products: as incompatibilities might be caused – depending on the antivirus version used in production – please check [15] and [16].

For a more comprehnsive list with official security advisories of affected vendors please check [21].

References

[1] https://meltdownattack.com/meltdown.pdf

[2] https://spectreattack.com/spectre.pdf

[3] https://googleprojectzero.blogspot.be/2018/01/reading-privileged-memory-with-side.html

[4] https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

[5] https://developer.arm.com/support/security-update

[6] https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/

[7] http://www.amd.com/en/corporate/speculative-execution

[9] https://access.redhat.com/security/vulnerabilities/speculativeexecution

[10] https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/

[11] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

[12] https://support.google.com/faqs/answer/7622138

[13] https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

[14] https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/

[15] https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

[16] https://docs.google.com/spreadsheets/u/1/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?sle=true#gid=0

[17] https://www.pcworld.com/article/3245790/mobile/spectre-cpu-faq-phones-tablets-ios-android.html

[18] https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html

[19] https://github.com/speed47/spectre-meltdown-checker

[20] https://support.apple.com/en-us/HT208394

[21] https://meltdownattack.com