SA-CPU-20180110-001: Multiple Vulnerabilities in CPU

Publication Date: 2018-01-10
Last Update: 2018-01-10
Version: V1.0
Severity: Important

Description

This advisory is in response to Google Project Zero's publication [1] of novel information disclosure attacks that combines CPU speculative execution with side channels. The vulnerabilities were published on the 3rd January, 2018.

- Bounds check bypass (CVE-2017-5753; also known as Spectre [2])
- Branch target injection (CVE-2017-5715; also known as Spectre [2])
- Rogue data cache load (CVE-2017-5754; also known as Meltdown [3])

Impact

Successful exploitation of these vulnerabilities allows a local user to read arbitrary memory by executing specially crafted code and observing changes of the CPU caches.

Affected Products

To our current knowledge following products are affected by Spectre (CVE-2017-5753 and CVE-2017-5715), in particular devices equipped with an ARM Cortex-A8 [5, 4]:

- Series PFC100 (750-81xx/xxx-xxx)
- Series PFC200 (750-82xx/xxx-xxx)
- Series e!DISPLAY 7300T

Series 750-8xx and 750-3xx are not vulnerable to Spectre attacks.

There are currently no known devices which are vulnerable by Meltdown (CVE-2017-5754) according to [6].

Vulnerability Characterization

The vulnerabilities reported affect a wide range of different CPU manufactures like Intel, AMD and ARM. The Issues identified facilitate the way CPU optimize performance by speculatively executing code in advance. There are three different variants which can be exploited by a local user.

The first two variants are CVE-2017-5753 (“bounds check bypass”) and CVE-2017-5715 (“branch target injection”), which are also known as Spectre, are based on the fact that the CPU is executing code speculatively in advance. By executing certain code sequences, it is possible to influence the CPU caches based on the value of the memory to be read, which then can be observed, i.e. establish a side-channel. Further information can be found in [1, 2, 4].

The latter variant is CVE-2017-5754 (“Rogue data cache load”), also known as Meltdown. In this case the CPU is executing speculative instructions without enforcing memory isolation which can be used to influence the caches of the CPU to gain knowledge of the memory content, i.e. establish a side-channel. Further information can be found in [1, 3, 4].

All three vulnerabilities have in common that it is required that an attacker has local access to the device and must be able to execute code [1, 2, 3]. Furthermore it is required, for Spectre (variant 1 and 2), that there exists a certain chain of instructions (gadgets) within the target process [1, 2, 3]. These gadgets, to current knowledge, are not found often in normal code and thus it is assumed practical exploitation requires an interpreter or JIT engine to forge these gadgets in the victim process as shown by the Proof of Concept of Google Project Zero [1].

CVE-2017-5753

- Severity: Important
- CVSS Base Score: 5.6
- CVSS3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
- Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVE-2017-5715

- Severity: Important
- CVSS Base Score: 5.6
- CVSS3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVE-2017-5754

- Severity: Important
- CVSS Base Score: 5.6
- CVSS3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

Solution

The issues are still under ongoing investigation. Please check the advisory for updates frequently.

Mitigation

- Restrict network access to the device.
- Do not directly connect the device to the internet.
- Restrict the number of users, with access to the device, to a minimum.
- Change the default passwords of devices.
- Do not install software from untrusted sources.

Additional Resources

[1] https://googleprojectzero.blogspot.de/2018/01/reading-privileged-memory-with-side.html
[2] https://spectreattack.com/spectre.pdf
[3] https://meltdownattack.com/meltdown.pdf
[4] https://developer.arm.com/support/security-update
[5] https://e2e.ti.com/support/arm/sitara_arm/f/791/t/654938
[6] https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

Disclaimer

http://global.wago.com/en/wago/impressum/software-user-agreement/index.jsp