Vulnerability of Speculative Processors to Cache Timing Side-Channel Mechanism

Based on the recent research findings from Google on the potential new cache timing side-channels exploiting processor speculation also known as Spectre and Meltdown, Beijer Electronics have comprised information of affected product and recommendations to mitigate the issue.

Cache timing side-channels are a well-understood concept in the area of security research and therefore not a new finding. However, this side-channel mechanism could enable someone to potentially extract information that otherwise would not be accessible to software from processors that are performing as designed.

What are the attack mechanisms?

There are three main variants of the exploits, as detailed by Google in their blogpost, that explain in detail the mechanisms:

- Spectre
  - Variant 1: bounds check bypass (CVE-2017-5753)
  - Variant 2: branch target injection (CVE-2017-5715)
- Meltdown
  - Variant 1: rogue data cache load (CVE-2017-5754)

The basic difference between Spectre and Meltdown is that Spectre can be used to manipulate a process into revealing its own data. On the other hand, Meltdown can be used to read privileged memory in a process's address space which even the process itself would normally be unable to access (this includes data belonging to the kernel or other processes).

What Beijer Electronics products are affected?

A list of active Beijer products that are affected can be found below.

	Spectre	Meltdown
PWS	No	No
EXTER	No	No
QTERM	No	No
iX TxA	No	No
iX TxB	Yes	Yes
PPC TxB	Yes	Yes
PPC TxBR	Yes	Yes
iX TxBR	Yes	Yes
iX TxC	Yes	Yes
PPC TxC	Yes	Yes
X2 base	No	No
X2 pro	Yes	No
X2 control	Yes	No
X2 motion	Yes	No
X2 marine	Yes	No
X2 extreme	Yes	No

Affected products and risks

Risks introduced

In normal operation, iX is an open system that allows for running programs with full privileges with no OS level user management. All code is run with a privileged OS user. Meaning if malicious code is run on the system it will have full access to the data contained in the system.

The speculative Processors to Cache Timing Side-Channel Mechanism introduces the possibility to have remote code executed using JavaScript loaded into the browser to gain access to data located on the panel.

Is my data at risk?

These exploits, when used for malicious purposes, have the potential to improperly gather sensitive data. Current information show that these exploits do not have the potential to corrupt, modify or delete data.

Are we aware of any real-world usage of these new exploits?

The researchers demonstrated a proof of concept. We are not aware of any malware based on these exploits.

Will performance be impacted by the operating system mitigations?

The OS mitigations released so far for Windows 7 has been shown to cause performance degradation due to the nature of the mitigation. The amount of reduction in performance depends on your typical work load. For iX specific applications, we do not expect significant performance impact and we will do performance tests in the upcoming iX 2.40 release.

General security recommendations

Always apply the latest software update provided by Beijer Electronics or the OS supplier for full PC systems.

Do not allow physical access to your devices ports for not authorized personnel.

Only allow web browser to browse know sites and do not allow arbitrary users to change URL.

iX TxB, iX TxBR

CPU family: Intel® Atom™ Processor E Series and Intel® Atom™ Processor Z

Operating system: Microsoft Windows CE6.0

Affected by both Spectre and Meltdown. Currently no solution for this is provided by Microsoft.

Actions required: Our customers should be cautioned to only use the browser against trusted sites. Arbitrary users should not be able to change which site is being browsed etc.

PPC TxB, PPC TxBR

CPU family: Intel® Atom™ Processor E Series

Operating system: Microsoft Windows Embedded Standard 7

Affected by both Spectre and Meltdown. Microsoft has provided security fixes for these systems via Microsoft update. Beijer Electronics is working to implement, test and release new versions of the operating system when delivered to our customers.

Actions required: Our customers should apply the latest patches of the operating system using Windows update.

iX TxC and PPC TxC

CPU family: Intel® Celeron B810E, Intel® Core i7 2715QE

Operating system: Microsoft Windows Embedded Standard 7, Microsoft Windows 7 pro

Affected by both Spectre and Meltdown. Microsoft has provided security fixes for these systems via Microsoft update. Beijer Electronics is working to implement, test and release new versions of the operating system when delivered to our customers.

Actions required: Our customers should apply the latest patches of the operating system using Windows update.

X2 pro, X2 control, X2 motion, X2 marine, X2 extreme

CPU family: NXP iMX6, ARM Cortex-A9

Operating system: Microsoft Windows Embedded Compact 2013

Affected by Spectre only. Currently no solution for this is provided by Microsoft.

Actions required: Our customers should be cautioned to only use the browser against trusted sites. Arbitrary users should not be able to change which site is being browsed etc.

Ongoing actions at Beijer Electronics to mitigate the vulnerability

- We continuously work with our Operating system provider, Microsoft, to receive mitigations for the security issue. When Microsoft provides updated we will implement these in our products.
- We are working to implement, test and release new versions of the Windows 7 based operating system to have the delivered to our customers with the latest patches installed

External Resources

- https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html
- https://developer.arm.com/support/security-update
- https://support.microsoft.com/da-dk/help/4073757/protect-your-windows-devices-against-spectre-meltdown