Advisory 2019-01: Spectre-V2 and impact on application performance as well as TwinCAT compatibility

Publication Date	03/14/2019 (Mar. 13th 2019)
Last Update	03/09/2021 (Mar. 09th 2021)
Current Version	1.4
Relevance	MEDIUM
Related CVE	CVE-2017-5715, CVE-2018-3639

Summary

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 [2]. Updates for Beckhoff components are available.

Updated systems need to be re-evaluated regarding their application performance.

By default, Beckhoff Images provide a medium security level for respecting the performance requirements of our customers.

Appearance

Application performance can be reduced and must be re-evaluated for suffient application performance of the affected system with the BIOS versions listed below in combination with Windows updates as of 2018/04.
Upcoming Microsoft hotfixes may also include these microcode updates making a BIOS update obsolete.
Please note that for all patched devices the default setting with Beckhoff's images is medium security. Please consider raising the security level if needed as described with the solution below. This hint will become general hardening step within Beckhoff's Guideline IPC Security (see https://www.beckhoff.com/secguide).

Device	*CPU*	*BIOS*
CBxx64	Skylake	v1.11, v1.12, v1.15, v1.16 and v1.18 and later
CBxx64	Kabylake	v1.15, 1.16 and v1.18 and later
CBxx60/61	Haswell	v1.31 and later
CBxx63	Baytrail	v0.47 and later
CBxx55/56	Sandy Bridge	v1.70 and later
CX51x0	Baytrail	v0.76 and later
CX20x0	Sandy Bridge	v1.65 and later
CBxx68	Whiskey Lake	v0.08 and later
CBxx67	Coffe Lake (Refresh)	v0.17 and later
CX20x2	Broadwell	no update needed
CX20x3	AMD Ryzen V1000	no update needed
CX52x0	Baytrail	no update needed

Operating system	*Classification*	*Update Catalog*
Windows 7 for x86-based Systems	Monthly Rollup	KB4093118
Windows 7 for x64-based Systems	Monthly Rollup	KB4093118
Windows Embedded Standard 7 for x86-based Systems	Monthly Rollup	KB4093118
Windows Embedded Standard 7 for x64-based Systems	Monthly Rollup	KB4093118
Windows Server 2008 R2 for x64-based Systems	Monthly Rollup	KB4093118
Windows 10 Version 1607 for 32-bit Systems	Cumulative Update	KB4093120
Windows 10 Version 1607 for x64-based Systems	Cumulative Update	KB4093120
Windows Server 2016 for x64-based Systems	Cumulative Update	KB4093120

Description

Systems mentioned above 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 [2].

Beckhoff provides a BIOS update on demand against Spectre-V2. To determine the correct BIOS version contact the service department (service@beckhoff.com) by providing the serial number of the IPC.

As a result, software applications have lower performance when Spectre-V2 protection is enabled. This must be considered when upgrading.

Solution

Apply these BIOS and operating system updates as described above to fix Spectre-V2.

After such updates, the performance and security relevant settings can be set. Disabling the Spectre-V2 protection restores the performance to its default. The “Mitigate” setting ensures the high-performance with medium operating system security. Beckhoff will deliver the mitigate settings by default.

The following registry entries can be adapted according to the requirements:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]

Default protection (all Spectre-V2 protection active) => delete these entries, if existing:

- `FeatureSettingsOverride`
- `FeatureSettingsOverrideMask`

To enable default mitigations for CVE-2017-5715 (Spectre Variant 2) and CVE-2017-5754 (Meltdown)

- `FeatureSettingsOverride        REG_DWORD   0x00000000`
- `FeatureSettingsOverrideMask    REG_DWORD   0x00000003`

To disable mitigations for CVE-2017-5715 (Spectre Variant 2), default by Beckhoff images

- `FeatureSettingsOverride        REG_DWORD   0x00000001`
- `FeatureSettingsOverrideMask    REG_DWORD   0x00000003`

Beckhoff recommends to use at least TwinCAT 2 Build 2304 and TwinCAT 3.1 Build 4022.30 together with these patches. For an existing system that must receive Windows updates, but TwinCAT must not be updated for internal reasons, the microcode updates should be switched off with the following registration keys. This ensures that the microcode is compatible with older TwinCAT versions. These two registration keys deactivate protection against Spectre / Meltdown, even if the system appears to be protected by the installed patch.

- `FeatureSettingsOverride              REG_DWORD   0x00000003`
- `FeatureSettingsOverrideMask          REG_DWORD   0x00000003`

Microsoft provides more comprehensive information in [3].

Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

Additional Resources

[1] A general guideline for Beckhoff IPC Security:
http://download.beckhoff.com/download/Document/product-security/ipc_security_en.pdf

[2] Jann Horn (Google Project Zero), Werner Haas, Thomas Prescher (Cyberus Technology), Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology)
https://spectreattack.com/. 2018

[3] https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

History

V 1.4	03/09/2021	Added information for new devices to appearance
V 1.3	06/25/2019	Added information for OS patches incl. Micorcode
V 1.2	06/19/2019	Added pararaph for TwinCAT compability information
V 1.1	03/15/2019	Original wording adopted from [3], defaults corrected
V 1.0	03/14/2019	Publication