Advisory 2019-02: Microarchitectural Data Sampling (MDS) vulnerabilities

Publication Date	12/06/2019
Last Update	15/07/2019
Current Version	1.2
Relevance	MEDIUM
Related CVE	CVE-2018-12126, CVE-2018-12130, CVE-2018-12127, CVE-2019-11091

Summary

The vulnerability called Microarchitectural Data Sampling (MDS) allows processes to access memory of other processes.

Appearance

Beckhoff IPCs with Intel CPUs could be affected by the published vulnerability called Microarchitectural Data Sampling (MDS). Intel published a list of affected CPUs [1]. Microsoft published a list of Intel microcode updates [2].

Description

On Mai 14th, 2019 Intel published microcode updates for their CPUs. The description contains information about a side channel attack of processes for accessing memory of other processes. The scenario seems to be more applicable in case of Hyper-Threading turned on. Beckhoff delivers IPCs with hyper-threading turned off by default. Operating system updates are available for example for Windows 7 and Windows 10.

Please note that the kind of attack to leak memory from one process to another is unlikely an attack scenario for industry controllers.

Solution

Beckhoff has evaluated the patches from Microsoft for use with Beckhoff TwinCAT (TwinCAT 3.1 Build 4022.30 and TwinCAT 2 Build 2304) and found no real-time performance impacts.
Beckhoff takes this as an indication that applying these patches does not harm the real-time capabilities. However, Beckhoff cannot foresee all changes of the patch on all variations in the field.

Please note that this patch contains KB4494175 from Microsoft. For older TwinCAT versions, this means that the handling of Advisory 2019-01 [5] must be applied.

Install Microsoft operating system updates
Beckhoff recommends creating a backup before installing updates so that the previous status can be restored at any time. This can be achieved with the Beckhoff Service Tool:
https://www.beckhoff.com/english.asp?industrial_pc/bst.htm
The operating system update for Windows 10 can be retrieved from [3].
The operating system update for Windows 7 can be retrieved from [4].

Disclaimer: Beckhoff is not responsible for any side effects negatively affecting the real-time capabilities of your TwinCAT control application possibly caused by updates. Beckhoff offers update images with qualified performance for Beckhoff hardware from time to time. TwinCAT System Manager offers tools, which can be of assistance to verify real-time performance after update. Only administrators or IT experts should perform the backup and update procedure

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-securityincident@beckhoff.com
www.beckhoff.com

Mitigation

If the solution is not applicable due to own tests, Beckhoff recommends to

- Minimize the likelihood by disabling Hyper-Threading.
  Please note that Beckhoff switches off Hyper-Threading by default on Beckhoff controllers due to real-time impact. Turning off Hyper-Threading may reduce the overall performance of user mode programs.

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] Intel publication:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

[2] Microsoft publication
https://support.microsoft.com/en-us/help/4494175/kb4494175-intel-microcode-updates

[3] https://www.catalog.update.microsoft.com/Search.aspx?q=KB4494175

[4] https://www.catalog.update.microsoft.com/Search.aspx?q=KB4499175

[5] Beckhoff Advisory 2019-01: Spectre-V2 and impact on application performance as well as TwinCAT compatibility https://download.beckhoff.com/download/Document/product-security/Advisories/advisory-2019-001.pdf

History

V 1.0	17/05/2019	Publication
V 1.1	29/05/2019	Test Results for TwinCAT compatibility added
V 1.2	15/07/2019	Added detailed TwinCAT versions of tests

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-securityincident@beckhoff.com
www.beckhoff.com