Security Advisory
Meltdown / Spectre

1 Advisory Information

Advisory ID: BOSCH-SA-879267
Published: 23 Jan 2018
Last Updated: 06 Feb 2018

2 Summary / Description

Meltdown and Spectre can be used to steal sensitive information. Basic measures to protect against malware are described in the DC Security-guideline. According to the actual state of knowledge embedded systems like CML75 only have a higher risk of vulnerability in case the device is additionally infected with malicious code. Unpatched Windows based systems need to undergo a risk assessment to find out, if sensitive data are being processed. If this is the case, we recommend to operate the system in a closed network until an appropriate patch is available.

The Windows-Security-Patches [5] for the risks Meltdown and Spectre seriously compromise the usability and functionality of the Bosch Rexroth engineering- and operating software IndraWorks. It prevents the start of internal service programs and dialog fields as well as the communication with controls and drives. Reason for that is a mistake on part of Microsoft [6]. Microsoft is working on a solution. We demand, **not** to in-stall these patches [5] on devices, which use IndraWorks. The installation of the patches through automatic updates needs to be prevented in cooperation with the responsible IT specialists. Instead, it has to be waited until an accurate patch from Microsoft is available.

The device is to be rated as unsecure until an accurate patch has been installed, and will therefore be vulnerable to the risks of Spectre / Meltdown in the meantime. Further operation of unsecure devices has to be coordinated with the IT specialists. We recommend to regularly check the information pages on Meltdown and Spectre [1] for the availability of recent bug-fix solutions for the Known Issue (CoInitializeSecurity) [6].

In case the patch has already been installed, the possibility to uninstall or rollback needs to be clarified in cooperation with the responsible IT specialists. Uninstalling or rollback contains the risk that the affected computer is out of order afterwards. It is highly recommended to safe data before uninstalling the patches.

Generally, all measures described in the DC Security-guideline should be implemented, e.g. segmentation of the network.

2.1 Update 06 Feb 2018

The Windows-Security-Patches [1] for the risks Meltdown and Spectre seriously compromise the usability and functionality of the Bosch Rexroth engineering- and operating software IndraWorks. It prevents the start of internal service programs and dialog fields as well as the communication with controls and drives. Reason for that is a mistake on part of Microsoft [1].

This malfunction does only affect the operating systems Windows 8 and Windows 10. The operating system Windows 7 is not, like we originally published, affected.

As a correction, Microsoft already published new error patches for some variants of the operating systems Windows 8 und Windows 10. We recommend to apply the security patches for Meltdown and Spectre only when the relevant additional bug fixes will be available. This is the only way to eliminate the security problem as well as to ensure the proper use of IndraWorks with relevant PCs or HMI devices.

Please note, the device is to be rated as unsecure until an accurate patch has been installed and will therefore be vulnerable to the risks of Spectre / Meltdown in the meantime. Further operation of unsecure devices has to be coordinated with the IT specialists.

Overview and relation of relevant patches – see below:

Microsoft security patches to fix Meltdown / Spec-tre problem				**Additional Microsoft Patches to ensure compatibility with Rexroth IndraWorks**
designation	publised	affected Windows version		designation / availability
KB4056888	Jan 3 2018	Windows 10 Version 1511 (OS Build 10586.1356)		KB4075200*
KB4056890	Jan 3 2018	Windows 10 Version 1607 Windows Server 2016 Windows 10 Mobile (OS Build 14393.2007)		KB4057142
KB4056891	Jan 3 2018	Windows 10 Version 1703 (OS Build 15063.850)		KB4057144
KB4056892	Jan 3 2018	Windows 10 version 1709 (OS Build 16299.192)		KB4073291 (32-Bit System) KB4073290 (64-Bit System)
KB4056893	Jan 3 2018	Windows 10 Enterprise (OS Build 10240.17738)		KB4075199*
KB4056896	Jan 4 2018	Windows Server 2012 Standard		KB4057402*
KB4056895	Jan 8 2018	Windows 8.1, Windows Server 2012 R2 Standard		KB4057401*
KB4056898	Jan 3 2018	Windows 8.1, Windows Server 2012 R2 Standard		KB4057401*
KB4056897	Jan 3 2018	Windows Server 2008 R2 Service Pack 1 Windows 7 Service Pack 1		not required Windows 7 not affected

Note: the relevant Windows version can be identified with the commands "ver" or "winver" entered at the Windows command line.

*You find a download file for Windows 10 32-bit-system — marked as X86 in the filename —and for Windows 10 64-bit-system marred with X64 in the file name.

We recommend to regularly check the information pages on Meltdown and Spectre [1] for the availability of recent bug-fix solutions for the Known Issue (CoInitializeSecurity) [6].

3 Additional Resources

[1] https://meltdownattack.com
[2] https://isc.sans.edu/diary/rss/23197
[3] https://developer.arm.com/support/security-update
[4] https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html
[5] KB4056891 (Windows 10 System Version 1703 Hotfix)
KB4056892 (Windows 10 System Version 1709 Hotfix)
KB4056893 (Windows 10 System Version 1705 Hotfix)
[6] https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892
(see also "Known Issues", CoInitializeSecurity)

For further questions please contact your local sales contact person.

4 Revision History

23 Jan 2018: Initial Publication
06 Feb 2018: Update product information