

**Memo**Lohr am Main  
2018-01**Important product information for Bosch Rexroth IndraWorks Engineering**

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 [2]. Microsoft is working on a solution. We demand, not to install these patches [1] 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 [3] for the availability of recent bug-fix solutions for the Known Issue (ColnitalizeSecurity) [2].

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.

## Sources:

[1] KB4056891 (Windows 10 System Version 1703 Hotfix)  
KB4056892 (Windows 10 System Version 1709 Hotfix)  
KB4056893 (Windows 10 System Version 1705 Hotfix)

[2] <https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892>  
(siehe "Known Issues", ColnitalizeSecurity)

[3] <https://meltdownattack.com/>

For further questions please contact your local sales contact person.