Rexroth
Bosch Group

Memo

Lohr am Main
2018-01

General Information on Meltdown / Spectre

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.

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

Together with partners, Bosch Rexroth is working on the identification of appropriate counter measures and their implementation as fast as possible.

Quellen:
https://meltdownattack.com
https://isc.sans.edu/diary/rss/23197
https://developer.arm.com/support/security-update
https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

For further questions please contact your local sales contact person.