Rexroth
Bosch Group

Memo

Lohr am Main
2018-01

Allgemeine Informationen zu Meltdown / Spectre

Meltdown und Spectre können zum Ausspähen von Daten genutzt werden. Grundsätzliche Maßnahmen zum Schutz gegen Schadsoftware sind im Security-Leitfaden dokumentiert. Auf Embedded Systemen wie der IndraControl CML75, ist nach aktuellem Kenntnisstand nur dann ein höheres Risiko vorhanden, wenn zusätzlich potentieller Schadcode auf dem Gerät selbst eingebracht wird.

Nicht gepatchte windowsbasierte Systeme sind einer Risikobeurteilung zu unterziehen, ob auf ihnen sensitive Daten verarbeitet werden. Wenn sensitive Daten verarbeitet werden, dann ist es beispielsweise eine sinnvolle Maßnahme das System in einem abgeschlossenen Netzwerk zu betreiben, bis ein geeigneter Patch zur Verfügung steht.

Generell sollten die im Security-Leitfaden aufgeführten Maßnahmen, z. B. eine Netzwerksegmentierung, umgesetzt werden.

Bosch Rexroth arbeitet zusammen mit seinen Partnern aktiv daran mögliche Handlungspunkte zu identifizieren und diese falls notwendig schnellst möglich umzusetzen.

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

Für Fragen wenden Sie sich bitte an Ihren zuständigen Vertrieb.