Rexroth
Bosch Group

Lohr am Main
2017-05-29

Memo

Gefährdung Rexroth HMI-Produkte durch WannaCry Ransomware

Potentiell gefährdete Geräte / Systeme

Für Industrie-PC und Embedded-PC Geräte mit Windows-Betriebsystemen Windows XP, Windows 7 und Windows 10 und einem Betriebsystemstand älter als März 2017 besteht eine Sicherheitsanfälligkeit durch Remotecode-ausführung über SMB (Quelle: https://technet.microsoft.com/de-de/library/security/ms17-010.aspx).

Diese Anfälligkeit wird aktuell durch die Ransomware „WannaCry“ genutzt um Schadsoftware zu verbreiten und Daten betroffener Systeme zu verschlüs-seln.

Potentiell gefährdet sind Produkte der Rexroth Gerätefamilien

- IndraControl VPB
- IndraControl VPP
- IndraControl VSP
- IndraControl VEP
- IndraControl VEH

mit nachfolgend aufgeführter Betriebssystem-Firmware

Windows 10 IoT Enterprise LTSB 2015

- R911375308 FWA-VP3***-W10-01VRS-A0
- R911376378 FWA-VP4***-W10-01VRS-A0
- R911375475 FWA-VEP*06-W10-01VRS-D0

Windows Embedded Standard 7

- R911172607 FWA-VP3***-W7*-01VRS-A0-OEM
- R911172608 FWA-VP3***-W7*-01VRS-A0-OEM A1
- R911338555 FWA-VP3***-W7*-01VRS-A0-OEM A1 32
- R911376435 FWA-VP4***-W7*-01VRS-A0-OEM
- R911377579 FWA-VP4***-W7*-01VRS-A0-OEM A1
- R911377580 FWA-VP4***-W7*-01VRS-A0-OEM A1 32
- R911337389 FWA-VEP*05-W7*-01VRS-D0-A* 32
- R911370518 FWA-VEP*06-W7*-01VRS-D0-A4 32

Windows 7 Ultimate

- R911338554 FWA-VP3***-W7U-01VRS-A0-OEM A1
- R911346128 FWA-VP3***-W7U-01VRS-A0-OEM A1 32

- R911377581 FWA-VP4***-W7U-01VRS-A0-OEM A1
- R911377582 FWA-VP4***-W7U-01VRS-A0-OEM A1 32

Windows XP
- R911172447 FWA-VS3VP3-WXP-03VRS-A0-OEM
- R911172448 FWA-VS3VP3-WXP-03VRS-A0-OEM A1

Windows XPe
- R911334113 FWA-VEP*04-XPE-01VRS-D0-A*
- R911324056 FWA-VEP*04-XPE-01VRS-D0-C*
- R911172171 FWA-VEH*02-XPE-01VRS-D0-A*
- R911337390 FWA-VEP*05-XPE-01VRS-D0-A*

Sowie die Schraubsteuerung CS351 Variante 0608PE1977 mit integrierter Rechnerkarte auf Basis Windows XP.

Infektion und Ausbreitung der Ransomware

Eine Infektion der Geräte mit der o.g. Ransomware kann durch Ausführen entsprechend infizierter Daten (Mail-Anhänge, aktive Office-Dateien, ausführbare Programme) oder auch durch Betrieb in einem Netzwerk mit anderen infizierten Geräten erfolgen.

Empfohlene Maßnahmen

Wird ein HMI-Gerät lokal ohne Netzwerkanbindung betrieben, dann sind im Hinblick auf die Verbreitung von WannaCry keine weiteren Maßnahmen erforderlich.

Beim Betrieb von HMI-Geräten mit Vernetzung wird die Installation der von Microsoft im März 2017 bereitgestellten Sicherheits-Patches empfohlen:

Windows 10
- KB4012606

Windows 7 32 Bit und 64 Bit
- KB4012212
-

Windows XP und XPe
- KB4012598

Lohr am Main
2017-05-29

Sollte in einer vernetzten Umgebung keine Anpassung der Betriebssystemkonfiguration möglich sein und die oben aufgeführten Patches aus Kompatibilitätsgründen nicht eingespielt werden können, dann muss das System durch externe Maßnahmen (z.B. durch Blockieren der Kommunikation über die für WannaCry relevanten Ports 135, 137-139 und 445 mittels Hardware-Firewall) vom Netzwerk abgeschottet werden.

Allgemeine Sicherheitsmaßnahmen für vernetzte Anlagen

Um dauerhaft den störungsfreien Betrieb von Produktionsanlagen zu ermöglichen empfehlen wir die Einhaltung einiger grundlegender Prinzipien:

- Sichere Trennung von Steuerungs- und Anlagennetzen von anderen Netzen mittels entsprechender Netzwerkinfrastruktur.
- Im Anlagennetz nur die für Produktion erforderlichen Programme und Dienste nutzen und erlauben.
- Kein Einsatz mobiler Datenträger (USB-Sticks) im Anlagennetz.
- Auf die Verwendung von z. B. Office- und Mailprogrammen im Anlagennetz verzichten.
- PCs regelmäßig mit einem aktuellen Virenscanner überprüfen und absichern.

Zur Beantwortung weiterer Fragen und zur Unterstützung bei der Umsetzung von Sicherheitsmaßnahmen steht Ihnen unser Service unter der Telefonnummer **+49 9352 405060** gerne zur Verfügung.

Gez. Produktmanagement DC-IA/SPC