Von
DC-AE/PJ-APS

Bearbeiter
Dietmar Trappiel

Telefon-Durchwahl
+49 9352 18-5734

Lohr am Main
12.02.2019

**Memo**

Empfänger
z. K.

# Wichtige Produktinformationen für Bosch Rexroth IndraWorks Operation (WinStudio)

Die Bosch Rexroth Engineering- und Betriebssoftware IndraWorks stellt Winstudio für die Entwicklung von Visualisierungsanwendungen zur Verfügung. Winstudio beinhaltet die Technologie von InduSoft Web Studio. Am 04.02.2019 hat AVEVA Software, LLC. "("AVEVA"), der Hersteller von InduSoft Web Studio, ein Sicherheitsbulletin [1] mit Informationen über eine kritische Sicherheitslücke in Web Studio veröffentlicht. Diese Schwachstelle betrifft ebenfalls:

- Alle Projekte, die mit Winstudio-Versionen vor 7.4 SP1 erstellt wurden.
- Alle Projekte, die mit IndraWorks-Versionen vor 15V02 erstellt wurden.

In zukünftigen Versionen von WinStudio (ab 7.4 SP1) sowie IndraWorks (ab 15V02) ist diese Lücke geschlossen. Es wird daher empfohlen, zeitnah nach deren Erscheinen auf diese Versionen zu aktualisieren.

Für bestehende Projekte, für Anwendungsfälle in denen eine Aktualisierung nicht möglich ist, sowie für die Übergangsphase wird eine der nachfolgenden Maßnahmen empfohlen. Abhängig von der gewählten Maßnahme wird die Lücke geschlossen oder das Ausnutzen der Lücke erschwert.

- Deaktivierung des TCP/IP-Servers. Hierdurch wird die Lücke *geschlossen*. Achtung: Nach dem Deaktivieren ist keine Verbindung per Web Thin Client oder Secure Viewer mehr möglich!

- Blockade der Ports 1234 (TCP) bzw. 51234 (TCP): Durch geeignete Infrastrukturmaßnahmen kann der Zugriff auf die Ports betroffener Geräte eingeschränkt werden. Diese Maßnahme *erschwert die Ausnutzung* der Lücke. Achtung: Abhängig von der Umsetzung ist auch in diesem Fall möglicherweise keine Verbindung per Web Thin Client oder Secure Viewer mehr möglich.

Von
DC-AE/PJ-APS

Bearbeiter
Dietmar Trappiel

Telefon-Durchwahl
+49 9352 18-5734

Lohr am Main
12.02.2019

Memo

Allgemein wird dringend empfohlen, die in der Bosch Rexroth Sicherheitsrichtlinie beschriebenen Maßnahmen umzusetzen, z.B. die Segmentierung von Netzwer-ken (Siehe dazu „Security-Leitfaden_DE“).

Weitere detaillierte technische Informationen über die Schwachstelle finden Sie unter [1], [2].

Quellen:
[1] Quelle Indusoft /AVEVA:
https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec133.pdf?hsLang=en

[2] PSIRT Information:
https://psirt.bosch.com/