By
DC-AE/PJ-APS

Author
Dietmar Trappiel

Phone extension
+49 9352 18-5734

Lohr am Main
12/02/2019

Memo

Recipient

Important Product Information for Bosch Rexroth IndraWorks Operation (WinStudio)

IndraWorks, the Bosch Rexroth Engineering and operating software, provides WinStudio to develop visualization applications. WinStudio contains the InduSoft Web Studio technology. On February 4, 2019 , AVEVA Software, LLC. "("AVEVA"), the InduSoft Web Studio manufacturer published a **security bulletin** [1] containing information about a critical security vulnerability in Web Studio. This vulnerability also affects:

- all projects created with Winstudio versions prior to 7.4 SP1.
- all projects created with IndraWorks versions prior to 15V02.

In future versions of WinStudio (from 7.4 SP1) and IndraWorks (from 15V02), this security vulnerability is fixed. Thus, it is recommended to update your versions to the versions mentioned above as soon as they have been published.

For existing projects, for use cases in which an update is not possible as well as during the transition phase, one of the following measures are recommended. Depending on the selected measure, the security vulnerability is fixed and taking advantage of the vulnerability is complicated.

- Disabling the TCP/IP server. The vulnerability is *fixed*. Caution: After the server has been disabled, it is not possible anymore to establish a connection via the Web Thin Client or via Secure Viewer!

- Disabling the 1234 (TCP) or 51234 (TCP) ports: Suitable measures regarding the infrastructure can limit the access to ports of affected devices. This measure *complicates taking advantage* of the vulnerability. Caution: Depending on the implementation, it might not be possible anymore to establish a connection via the Web Thin Client or via Secure Viewer.

rexroth
A Bosch Company

By	Author	Phone extension	Lohr am Main
DC-AE/PJ-APS	Dietmar Trappiel	+49 9352 18-5734	12/02/2019

Memo

Bosch Rexroth strongly recommends to implement the measures described in the Bosch Rexroth Safety directive; e.g. network segmentation (see “Security-Manual_EN”).

For more detailed technical information about the vulnerability, refer to [1], [2].

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

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

Fehler! Verweisquelle konnte nicht gefunden werden. 2 **Fehler! Verweisquelle konnte nicht gefunden werden.**