

Von  
DC-AE/ESW2PJ-  
APS

Bearbeiter  
Dietmar Trappiel

Telefon-Durchwahl  
+49 9352 18-  
11945734

Lohr am Main  
31.10.2018

## Memo

Empfänger  
z. K.

# Important product information for Bosch Rexroth IndraWorks Operation (WinStudio)

The Bosch Rexroth engineering- and operating software *IndraWorks* provides *WinStudio* for the development of visualization applications. WinStudio includes technology from InduSoft Web Studio. On 10/31/2018 AVEVA Software, LLC. ("AVEVA"), the vendor of InduSoft Web Studio, published a security bulletin [2] with 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

Users are advised to review existing WinStudio projects and to apply the following security related settings in case they have not been applied yet:

1. Set a strong Master Project password.
2. Set a strong password for the built-in account. By default, the built-in account is named Guest.
3. Set strong passwords for all other non-built-in accounts.

In future versions of WinStudio 7.4 SP1 / IndraWorks 15V02, the project wizard will include these settings by default for all new projects.

Additionally, it is strongly advised to implement the measures, which are described in the DC Security Guideline [1], e.g. segmentation of networks.

Please see [2], [3] for further detailed technical information about the vulnerability.

Von  
DC-AE/ESW2PJ-  
APS

Bearbeiter  
Dietmar Trappiel

Telefon-Durchwahl  
+49 9352 18-  
11945734

Lohr am Main  
31.10.2018

Memo

Sources:

[1]

[https://md.boschrexroth.com/modules/BRMV2PDFDownload-intra-net.dll/R911342562\\_05.pdf?db=brmv2&lvid=1207302&mvid=13666&clid=1&sid=EB65E98BA5F4D612EC49A33F130E80FF.borex-tc&sch=M&id=13666,1,1207302](https://md.boschrexroth.com/modules/BRMV2PDFDownload-intra-net.dll/R911342562_05.pdf?db=brmv2&lvid=1207302&mvid=13666&clid=1&sid=EB65E98BA5F4D612EC49A33F130E80FF.borex-tc&sch=M&id=13666,1,1207302)

[2] Source Indusoft /AVEVA:

[https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin\\_LFSec130.pdf](https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec130.pdf)

[3] PSIRT information:

<https://psirt.bosch.com/>