Security Advisory
Bosch Rexroth IndraWorks Operation (WinStudio)

1 Advisory Information

Advisory ID: BOSCH-2018-1101
Published: 27 Nov 2018
Last Updated: 27 Nov 2018
CVSSv3 Base Score:

- CWE-121 : Stack-based Buffer Overflow
  - CVSS 3.0: 9.8, CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CWE-258 : Empty Password in Configuration

2 Summary

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 [1] with information about a critical security vulnerability in Web Studio. This vulnerability also affects all projects created with WinStudio version prior to 7.4 SP1 and IndraWorks versions prior to 15V02.

3 Affected Products

- All projects created with WinStudio versions prior to 7.4 SP1
- All projects created with IndraWorks versions prior to 15V02

4 Solution

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

- Set a strong Master Project password.
- Set a strong password for the built-in account. By default, the built-in account is named Guest.
- 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, e.g. segmentation of networks.

Please see [1] for further additional information about the vulnerability.

5 Vulnerability Details

A remote user could send a carefully crafted packet to exploit a stack-based buffer overflow vulnerability during tag, alarm, or event related actions such as read and write, with potential for code to be executed. If remote communication security was not enabled, or a password was left blank, a remote user could send a carefully crafted packet to invoke an arbitrary process, with potential for code to be executed. The code would be executed under the privileges of the runtime user.

- CWE-121 : Stack-based Buffer Overflow
  - CVSS 3.0: 9.8, CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CWE-258 : Empty Password in Configuration

Vulnerability classification has been performed using the CVSSv3 scoring system (http://www.first.org/cvss/) . The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

6 Additional Resources

[1] AVEVA Security Bulletin LFSEC00000130

7 Revision History

27 Nov 2018: Initial Publication