Security Advisory

Bosch Rexroth IndraWorks Operation (WinStudio)

1 Advisory Information

Advisory ID: BOSCH-2019-0201
Published: 18 Feb 2019
Last Updated: 18 Feb 2019
CVSSv3 Base Score:

- CWE-306 : Missing Authentication for Critical Function
  - 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-99 : Improper Control of Resource Identifiers ('Resource Injection')

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 02/04/2019 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

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.

Additionally, it is strongly advised to implement the measures, which are described in the Bosch Rexroth Security Manual, e.g. segmentation of networks.

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

5 Vulnerability Details

An unauthenticated remote user could use a specially crafted database connection configuration file to execute an arbitrary process on the Server Machine. The code would be executed under the privileges of the InduSoft Web Studio or InTouchEdge HMI runtime and could lead to a compromise of the InduSoft Web Studio or InTouch Edge HMI server machine.

- CWE-306 : Missing Authentication for Critical Function
  - 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-99 : Improper Control of Resource Identifiers (‘Resource Injection’)

Vulnerability classification has been performed using the CVSSv3 scoring system . 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 LFSEC00000133

7 Revision History

18 Feb 2019: Initial Publication