Security Advisory
FTP Backdoor for Rexroth Fieldbus Couplers S20 and Inline

1 Advisory Information

Advisory ID: BOSCH-SA-428397
Published: 30 Apr 2021
Last Updated: 30 Apr 2021

2 Summary

On some Fieldbus Couplers, there is a hidden, password-protected FTP area for the root directory.

3 Affected Products

- R911173318 - Rexroth S20-S3-BK+ < AE1
- R911173359 - Rexroth S20-PN-BK+ < AB1
- R911173906 - Rexroth S20-EC-BK < AD1
- R911173905 - Rexroth S20-ETH-BK < AC1
- R911173904 - Rexroth S20-EIP-BK < AC1
- R911170875 - Rexroth R-IL S3 BK DI8 DO4-PAC- all versions
- R911171944 - Rexroth R-IL PN BK DI8 DO4-PAC- all versions
- R911171726 - Rexroth R-IL ETH BK DI8 DO4 2TX-PAC - all versions

4 Solution

4.1 Compensatory Measures

If possible, protect your network by blocking access to FTP.

4.2 Apply DC Security Policy

When using the devices, it is strongly recommended to implement the measures for network segmentation described in the DC Security Policy (see "Security Guideline Electric Drives and Controls" [1]).

5 Additional Resources

[1] Bosch Rexroth Security Guideline Electric Drives and Controls:
   https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562

6 Revision History

30 Apr 2021: Initial Publication