Security Advisory

Multiple Vulnerabilities in 3S CODESYS Runtime in Rexroth PRC7000

1 Advisory Information

Advisory ID: BOSCH-SA-387388

CVE Numbers and CVSS v3.1 Scores:

- CVE-2019-18858
  - Base Score: 10.0 (Critical)
- CVE-2019-5105
  - Base Score: 7.5 (High)
- CVE-2019-9010
  - Base Score: 9.0 (Critical)
- CVE-2019-9012
  - Base Score: 7.5 (High)
- CVE-2019-9013
  - Base Score: 8.8 (High)
- CVE-2020-10245
  - Base Score: 10.0 (Critical)

Published: 16 Dec 2020

Last Updated: 16 Dec 2020

2 Summary

The PRC7000 welding timer sold by Bosch Rexroth AG contains a CODESYS Soft-PLC Runtime from 3S. The manufacturer published security reports [1] about several weaknesses. By exploiting those weaknesses, an attacker can cause denial-of-service conditions or acquire user credentials.

The vulnerabilities affect all firmware versions up to 1.11.3, and are fixed with the release of version 1.11.4.

3 Affected Products

- Rexroth PRC7000 <= 1.11.3

4 Solution and Mitigations

4.1 Firmware Update

If you determine that mitigating the vulnerabilities by applying network segmentation (see next section) is not sufficient for your use case, please get in contact with us via service.resistance-welding@boschrexroth.de. After evaluating your specific use case, we offer you one of the following solutions:

1. Update your product firmware to 1.11.4 or newer as soon as it is available
2. Provide a hotfix for your current firmware, which disables all network ports of the 3S CODESYS Runtime. The effort to provide this hotfix may vary depending on the firmware version. Please note that this may affect on-site service operations negatively.

We strongly suggest applying the mitigation described in the next section. Firmware version 1.11.4 will be available at the end of Q1/2021.

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 Manual Electric Drives and Controls” [2]).

5 Vulnerability Details

5.1 CVE-2019-18858

The Rexroth PRC7000 welding timer is affected by CVE-2019-18858.

CVE description: CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems,
has a Buffer Overflow.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 10.0 (Critical)

5.2 CVE-2019-5105

The Rexroth PRC7000 welding timer is affected by CVE-2019-5105.

CVE description: An exploitable memory corruption vulnerability exists in the Name Service Client functionality of 3S-Smart Software Solutions CODESYS GatewayService. A specially crafted packet can cause a large memcpy, resulting in an access violation and termination of the process. An attacker can send a packet to a device running the GatewayService.exe to trigger this vulnerability. All variants of the CODESYS V3 products in all versions prior V3.5.16.10 containing the CmpRouter or CmpRouterEmbedded component are affected, regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PLCnext, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control RTE V3, CODESYS Control RTE V3 (for Beckhoff CX), CODESYS Control Win V3 (also part of the CODESYS Development System setup), CODESYS Control V3 Runtime System Toolkit, CODESYS V3 Embedded Target Visu Toolkit, CODESYS V3 Remote Target Visu Toolkit, CODESYS V3 Safety SIL2, CODESYS Edge Gateway V3, CODESYS Gateway V3, CODESYS HMI V3, CODESYS OPC Server V3, CODESYS PLCHandler SDK, CODESYS V3 Simulation Runtime (part of the CODESYS Development System).

- Problem Type:
  - Memory corruption
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.3 CVE-2019-9010

The Rexroth PRC7000 welding timer is affected by CVE-2019-9010.
CVE description: An issue was discovered in 3S-Smart CODESYS V3 products. The CODESYS Gateway does not correctly verify the ownership of a communication channel. All variants of the following CODESYS V3 products in all versions prior to v3.5.14.20 that contain the CmpGateway component are affected, regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control V3 Runtime System Toolkit, CODESYS Gateway V3, CODESYS V3 Development System.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 9.0 (Critical)

5.4 CVE-2019-9012

The Rexroth PRC7000 welding timer is affected by CVE-2019-9012.

CVE description: An issue was discovered in 3S-Smart CODESYS V3 products. A crafted communication request may cause uncontrolled memory allocations in the affected CODESYS products and may result in a denial-of-service condition. All variants of the following CODESYS V3 products in all versions prior to v3.5.14.20 that contain the CmpGateway component are affected, regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control V3 Runtime System Toolkit, CODESYS Gateway V3, CODESYS V3 Development System.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

5.5 CVE-2019-9013

The Rexroth PRC7000 welding timer is affected by CVE-2019-9013.

CVE description: An issue was discovered in 3S-Smart CODESYS V3 products. The application may utilize non-TLS based encryption, which results in user credentials being insufficiently protected during transport. All variants of the following CODESYS V3 products in all versions containing the CmpUserMgr component are affected regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control RTE V3, CODESYS Control RTE V3 (for Beckhoff CX), CODESYS Control Win V3 (also part of the CODESYS Development System setup), CODESYS V3 Simulation Runtime (part of the CODESYS Development System), CODESYS Control V3 Runtime System Toolkit, CODESYS HMI V3.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.6 CVE-2020-10245

The Rexroth PRC7000 welding timer is affected by CVE-2020-10245.
CVE description: CODESYS V3 web server before 3.5.15.40, as used in CODESYS Control runtime systems, has a buffer overflow.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 10.0 (Critical)

5.7 Remark

Vulnerability classification has been performed using the CVSS v3.1 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] 3S CODESYS Security Reports:
https://www.codesys.com/security/security-reports.html

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

7 Revision History

16 Dec 2020: Initial Publication