Security Advisory
Denial of Service in PLC Runtime affecting Rexroth IndraMotion Products

1 Advisory Information

Advisory ID: BOSCH-SA-152060
CVE Numbers and CVSS v3.1 Scores:

- CVE-2019-5105
  - Base Score: 7.5 (High)
- CVE-2020-7052
  - Base Score: 7.1 (High)

Published: 16 Dec 2020
Last Updated: 16 Dec 2020

2 Summary

The control systems IndraMotion MTX, MLC and MLD sold by Bosch Rexroth contain technology from CODESYS GmbH. The manufacturer published security bulletins [1], [2] about a weakness in the communication interface of the PLC runtime. By exploiting these vulnerabilities, the control device can be put into a state in which network queries are no longer answered. To restore the device to a proper state, it must be restarted.

These vulnerabilities affect all available software versions of Rexroth IndraMotion MTX, MLC and MLD.

3 Affected Products

- Rexroth IndraMotion MTX
- Rexroth IndraMotion MLC
- Rexroth IndraMotion MLD

4 Solution and Mitigations

4.1 Use ctrlX CORE

A CODESYS version with resolved security issues is integrated in ctrlX CORE.

4.2 4.2 Apply DC Security Policy

It is strongly recommended to implement the measures for network segmentation described in the DC Security Policy (see “Security Manual Electric Drives and Controls” [3]), especially if the use of ctrlX CORE is not possible.

5 Vulnerability Details

5.1 CVE-2019-5105

Rexroth IndraMotion MTX, MLC and MLC are 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)

5.2 CVE-2020-7052

Rexroth IndraMotion MTX, MLC and MLC are affected by CVE-2020-7052.

CVE description: CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition.

- Problem Type:
  - n/a
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
  - Base Score: 7.1 (High)

5.3 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] Codesys Security Advisory ID 2020-01:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=

[2] Codesys Security Advisory ID 2020-02:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=

[3] 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