Security Advisory
Vulnerabilities in CODESYS V2 runtime systems

1 Advisory Information

Advisory ID: BOSCH-SA-475180
CVE Numbers and CVSS v3.1 Scores:

- CVE-2021-30186
  - Base Score: 7.5 (High)
- CVE-2021-30188
  - Base Score: 9.8 (Critical)
- CVE-2021-30195
  - Base Score: 7.5 (High)

Published: 09 Jul 2021
Last Updated: 09 Jul 2021

2 Summary

The control systems SYNAX, Visual Motion, IndraLogic, IndraMotion MTX, IndraMotion MLC and IndraMotion MLD contain PLC technology from CODESYS GmbH. The manufacturer CODESYS GmbH published a security bulletin [1] about a weakness in the protocol for the communication between the PLC runtime and clients. By exploiting the vulnerability, attackers can send crafted communication packets which may result in a denial of service condition or allow in worst case remote code execution.

3 Affected Products

- IndraMotion MLD <= MPH 17VRS
- IndraLogic <= 04VRS
- IndraMotion MLC <= 04VRS
- IndraMotion MTX 02VRS - 12VRS
- SYNAX 11VRS - 13VRS
- Visual Motion 11VRS

4 Solution and Mitigations

4.1 Use of Security Certified ctrlX CORE

Use of ctrlX CORE as security gateway for protection of the affected products or replace the affected products with ctrlX Core.

4.2 Compensatory Measures

If the solutions in 4.1 are not applicable, compensatory measures are recommended which mitigate the risk.. Always define such compensatory measures individually, in the context of the operational environment. Some measures are described in the “Security Guideline Electric Drives and Controls”, for example the network segmentation (please see [2]). In general, it is mandatory to implement the measures described in the “Security Guideline Electric Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2021-30186

CVE description: CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow.

- Problem Type:
  - CWE-787
- 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-2021-30188

CVE description: CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.3 CVE-2021-30195

CVE description: CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation.

- Problem Type:
  - CWE-125
- 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)

5.4 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 2021-06:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925890176ecd78&download

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

7 Revision History

09 Jul 2021: Initial Publication