Security Advisory

Vulnerability in the routing protocol of the PLC runtime

1 Advisory Information

Advisory ID: BOSCH-SA-350374
CVE Numbers and CVSS v3.1 Scores:

- CVE-2021-29242
  - Base Score: 7.3 (High)

Published: 19 May 2021
Last Updated: 19 May 2021

2 Summary

The control systems IndraMotion MTX, MLC and MLD and the ctrlX CORE PLC application contain PLC technology from Codesys GmbH. The manufacturer Codesys GmbH published a security bulletin [1] about a weakness in the routing protocol for the communication between the PLC runtime and clients. By exploiting the vulnerability, attackers can send crafted communication packets to change the routers addressing scheme and may re-route, add, remove or change low level communication packages.

On the ctrlX CORE PLC Runtime, an attacker might try to obfuscate the origin of the attacker's address and therefore cover up tracks by exploiting the vulnerability, or, in a worst case scenario, cause a temporary interruption in the communication to the PLC Runtime. No authentication bypass is possible. A restart of the PLC Runtime application does reset the application to a working state.

On IndraMotion MLC, MTX and MLD an attacker might act as a Man in the Middle by exploiting the vulnerability and therefore manipulate communication requests between the PLC runtime and clients. In the worst case scenario, this would allow to manipulate the PLC Runtime and/or read data without authorization.

The vulnerability currently affects all available software versions.

3 Affected Products

- ctrlX CORE PLC App <= 01V08
- IndraMotion MTX - all versions
- IndraMotion MLC - all versions
- IndraMotion MLD - all versions

4 Solution and Mitigations

4.1 Software Update to ctrlX CORE PLC App 01V10

ctrlX CORE PLC App Release 01V10 will include an updated release of the Codesys software stack which corrects the vulnerability Please update your crlX CORE installation to this release when it becomes available. Please contact your sales partner for instructions on how to retrieve the update.

For IndraMotion MLC, MTX or MLD the following options exist:

- Use of ctrlX CORE as security gateway for protection of IndraMotion MLC, MTX or MLD
- Use of ctrlX CORE instead of IndraMotion MLC, MTX or MLD

4.2 Compensatory Measures

Until updated releases are available or if the solutions described 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 possible measures are described in the “Security Guideline Electric Drives and Controls”, for example the network segmentation (please see [2]). In general, it is highly recommended to implement the measures described in the “Security Guideline Electric Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2021-29242

CVE description: CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router’s addressing scheme and may re-route, add, remove or change low level communication packages.

- Problem Type:
  - CWE-20
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
  - Base Score: 7.3 (High)

6 Additional Resources

[1] Codesys Security Advisory ID 2021-01:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&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

19 May 2021: Initial Publication