Security Advisory

Vulnerabilities in the communication protocol of the PLC runtime

1 Advisory Information

Advisory ID: BOSCH-SA-577411
CVE Numbers and CVSS v3.1 Scores:

- CVE-2022-22513
  - Base Score: 6.5 (Medium)
- CVE-2022-22514
  - Base Score: 7.1 (High)
- CVE-2022-22515
  - Base Score: 7.1 (High)
- CVE-2022-22517
  - Base Score: 7.5 (High)
- CVE-2022-22519
  - Base Score: 7.5 (High)

Published: 02 May 2022
Last Updated: 11 Oct 2022

2 Summary

The PLC application of the control systems ctrlX CORE, IndraLogic, IndraMotion MTX, IndraMotion MLC and IndraMotion MLD contains PLC technology from CODESYS GmbH. The manufacturer CODESYS GmbH published multiple security bulletins [1], [2], [3], [4], [5]. By exploiting the vulnerabilities in the protocol for the communication between the PLC runtime and clients, attackers can send crafted communication packets which may result in a stop of the web server communication of the PLC runtime or a temporary blocking of the communication to the PLC runtime.

3 Affected Products

- IndraLogic (all versions)
  - CVE-2022-22513 (affected only when user management is disabled)
  - CVE-2022-22514 (affected only when user management is disabled)
  - CVE-2022-22515 (affected only when user management is disabled)
  - CVE-2022-22517

- IndraMotion MLC (all versions)
  - CVE-2022-22513 (affected only when user management is disabled)
  - CVE-2022-22514 (affected only when user management is disabled)
  - CVE-2022-22515 (affected only when user management is disabled)
  - CVE-2022-22517

- IndraMotion MLD (all versions)
  - CVE-2022-22513 (affected only when user management is disabled)
  - CVE-2022-22514 (affected only when user management is disabled)
  - CVE-2022-22515 (affected only when user management is disabled)
  - CVE-2022-22517
- IndraMotion MTX (all versions)
  - CVE-2022-22513 (affected only when user management is disabled)
  - CVE-2022-22514 (affected only when user management is disabled)
  - CVE-2022-22515 (affected only when user management is disabled)
  - CVE-2022-22517
- ctrlX CORE PLC <= PLC-V-0116
  - CVE-2022-22515
  - CVE-2022-22517
  - CVE-2022-22519

4 Solution

4.1 Update to ctrlX CORE PLC 01V18

ctrlX CORE PLC 01V18 will include an updated CODESYS version which has fixed the vulnerability CVE-2022-22515.

4.2 Use of a Security Gateway

Use a security gateway, e.g. the ctrlX CORE, for the protection of the affected systems.

4.3 Compensatory Measures

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” [6], for example the network segmentation. In general, it is mandatory to implement the measures described in the “Security Guideline Electric Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2022-22513

CVE description: An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash.

- Problem Type:
  - CWE-476 NULL Pointer Dereference
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 6.5 (Medium)

5.2 CVE-2022-22514

CVE description: An authenticated, remote attacker can gain access to a dereferenced pointer contained in a request. The accesses can subsequently lead to local overwriting of memory in the CmpTraceMgr, whereby the attacker can neither gain the values read internally nor control the values to be written. If invalid memory is accessed, this results in a crash.

- Problem Type:
  - CWE-822: Untrusted Pointer Dereference
- 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 CVE-2022-22515

CVE description: A remote, authenticated attacker could utilize the control program of the CODESYS Control runtime system to use the vulnerability in order to read and modify the configuration file(s) of the affected products.

- Problem Type:
  - CWE-668 Exposure of Resource to Wrong Sphere
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N
  - Base Score: 7.1 (High)

5.4 CVE-2022-22517

CVE description: An unauthenticated, remote attacker can disrupt existing communication channels between CODESYS products by guessing a valid channel ID and injecting packets. This results in the communication channel to be closed.

- Problem Type:
  - CWE-334 Small Space of Random Values
- 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-2022-22519

CVE description: A remote, unauthenticated attacker can send a specific crafted HTTP or HTTPS requests causing a buffer over-read resulting in a crash of the webserver of the CODESYS Control runtime system.

- Problem Type:
  - CWE-126 Buffer Over-read
- 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)

6 Additional Resources

[1] CODESYS Security Advisory ID 2022-02:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17089&token=cc5041e24fc744a397a6f6e3b78200a40e6fcd53&download

[2] CODESYS Security Advisory ID 2022-03:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17090&token=6cd08b169916366df31388d2e7ba58e7bce93508&download

[3] CODESYS Security Advisory ID 2022-04:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17091&token=c450f8bbbd838c647d102f359356386c6ea5aeca&download

[4] CODESYS Security Advisory ID 2022-06:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download

[5] CODESYS Security Advisory ID 2022-07:
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17094&token=2fb188e2213c74194e81ba61ff99f1c68602ba4d&download

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

7 Revision History

11 Oct 2022: Updated the advisory - ctrlX CORE PLC
07 Jul 2022: Updated the advisory - ctrlX CORE PLC
02 May 2022: Initial Publication