Security Advisory
Multiple vulnerabilities in the web server

1 Advisory Information

Advisory ID: BOSCH-SA-741752
CVE Numbers and CVSS v3.1 Scores:

- CVE-2021-23855
  - Base Score: 8.6 (High)
- CVE-2021-23856
  - Base Score: 10.0 (Critical)
- CVE-2021-23857
  - Base Score: 10.0 (Critical)
- CVE-2021-23858
  - Base Score: 8.6 (High)

Published: 30 Sep 2021
Last Updated: 30 Sep 2021

2 Summary

The control systems series Rexroth IndraMotion MLC and IndraLogic XLC are affected by multiple vulnerabilities in the web server, which – in combination – ultimately enable an attacker to log in to the system.

- Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource, and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource.
- Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with the aforementioned vulnerability, this allows an attacker to subsequently login to the system

The control systems Rexroth IndraMotion MLC are affected by multiple further vulnerabilities in the web server.

- Information disclosure: The user and password data base are exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables
- Reflected Cross-Site-Scripting: The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's computer by sending the client a manipulated URL.

These vulnerabilities were discovered and reported by Matan Dobrushin and Eran Jacob from OTORIO Research

3 Affected Products

- IndraMotion MLC IndraMotion XLC
  - CVE-2021-23855
- IndraMotion MLC L20, L40
  - CVE-2021-23856
- IndraMotion MLC L20, L40 >= 12 VRS
  - CVE-2021-23857
  - CVE-2021-23858
- IndraMotion MLC L25, L45, L65, L75, L85, XM21, XM22, XM41 and XM42 IndraControl XLC >= 12 VRS
  - CVE-2021-23858
- IndraMotion MLC L25, L45, L65, L75, L85, XM21, XM22, XM41 and XM42 IndraMotion XLC >= 12 VRS
  - CVE-2021-23857

4 Solution

4.1 Use of a security gateway

Use of a security gateway, e.g. the ctrlX CORE, for the protection of the affected products or replace the affected products. The IndraMotion and IndraLogic series are not intended to be used in open networks and therefore requires protection by external devices.

4.2 Compensatory Measures

In general, compensatory measures are strongly advised 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 [1]). In general, it is mandatory to implement the measures described in the “Security Guideline Electric Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2021-23855

CVE description: The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables.

- Problem Type:
  - CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
  - Base Score: 8.6 (High)

5.2 CVE-2021-23856

CVE description: The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's computer by sending the client a manipulated URL.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- 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)

5.3 CVE-2021-23857

CVE description: Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system.

- Problem Type:
  - CWE-836 Use of Password Hash Instead of Password for Authentication
- 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)

5.4 CVE-2021-23858

CVE description: Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource, and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource.

- Problem Type:
  - CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
  - Base Score: 8.6 (High)

6 Additional Resources

[1] Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/de/de/myrexroth/media-directory-download?object_nr=R911342562

7 Revision History

30 Sep 2021: Initial Publication