Security Advisory

Vulnerability in SICK Flexi Soft Gateway

1 Advisory Information

Advisory ID: BOSCH-SA-164691
CVE Numbers and CVSS v3.1 Scores:

- CVE-2023-5246
  - Base Score: 8.8 (High)

Published: 24 Oct 2023
Last Updated: 24 Oct 2023

2 Summary

The SLC-0-GPNT00300 from Bosch Rexroth contains technology from SICK AG. The manufacturer has published a security bulletin [1] regarding an Authentication Bypass by Capture-replay. Exploiting the vulnerability would allow an unauthenticated attacker to login to the gateways by sending specially crafted packets and potentially impact the availability, integrity, and confidentiality of the devices.

3 Affected Products

- Rexroth SLC-0-GPNT00300
  - CVE-2023-5246
    - Version(s): all

4 Solution

4.1 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” [2], 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-2023-5246

CVE description: Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity, and confidentiality of the gateways via an authentication bypass by capture-replay.

- Problem Type:
  - CWE-294: (Authentication Bypass by Capture-replay)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

6 Additional Resources

[1] Third Party Supplier Advisory:
https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf

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

7 Revision History

24 Oct 2023: Initial Publication