Security Advisory
Vulnerability in the interface module SLC-0-GPNT00300

1 Advisory Information

Advisory ID: BOSCH-SA-894143
CVE Numbers and CVSS v3.1 Scores:
▶ CVE-2023-23444
   o Base Score: 7.5 (High)
Published: 04 Jul 2023
Last Updated: 04 Jul 2023

2 Summary

The SLC-0-GPNT00300 from Bosch Rexroth contains technology from SICK AG. The manufacturer has published a security bulletin [1] regarding the missing authentication for a critical function. Exploiting the vulnerability would allow an unauthenticated attacker to change the IP address of the device and affect the availability of the module.

3 Affected Products

▶ Rexroth SLC-0-GPNT00300 (all versions)
   o CVE-2023-23444

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-2023-23444

CVE description: Missing Authentication for Critical Function in SICK Flexi Classic and Flexi Soft Gateways with Partnumbers 1042193, 1042964, 1044078, 1044072, 1044073, 1044074, 1099830, 1099832, 1127717, 1069070, 1112296, 1051432, 1102420, 1127487, 1121596, 1121597 allows an unauthenticated remote attacker to influence the availability of the device by changing the IP settings of the device via broadcasted UDP packets.

▶ Problem Type:
   o CWE-306

▶ CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   o Base Score: 7.5 (High)

6   Additional Resources

[1] Third Party Supplier Advisory:
   https://www.sick.com/.well-known/csaf/white/2023/sca-2023-0003.pdf

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

7   Revision History

04 Jul 2023: Initial Publication