Security Advisory
Use of Telnet in the interface module SLC-0-GPNT00300

1 Advisory Information

Advisory ID: BOSCH-SA-387640
CVE Numbers and CVSS v3.1 Scores:

- CVE-2023-23451
  - Base Score: 9.8 (Critical)

Published: 28 Apr 2023
Last Updated: 28 Apr 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 availability of a Telnet interface for debugging.

The SLC-0-GPNT00300 provides a Telnet interface for debugging, which is enabled by factory default.
No password is set in the default configuration.
If the password is not set by the customer, a remote unauthorized adversary could connect via Telnet.
The adversary may use the debugging interface to subsequently gain access to the boot loader and in the worst case modify the firmware of the devices.

3 Affected Products

- Rexroth SLC-0-GPNT00300 (all versions)
  - CVE-2023-23451

4 Solution & Mitigations

4.1 Solution

Please make sure that you set a strong password for the Telnet protocol with a maximum length of 15 characters once the device is put into operation. Enter the following commands to change the Telnet password:

```
$ telnet <Gateway-IP-Address>
Password: <old password> [ Enter ]
passwd <utmost secure password, followed by [ Enter ]>
quit [ Enter ]

$ telnet <Gateway-IP-Address >
Password: <new password> [ Enter ]

Test if [ Enter ] still works and if the new password has been saved.
```

4.2 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-2023-23451

CVE description: The Flexi Classic and Flexi Soft Gateways SICK UE410-EN3 FLEXI ETHERNET GATEW., SICK UE410-EN1 FLEXI ETHERNET GATEW., SICK UE410-EN3S04 FLEXI ETHERNET GATEW., SICK UE410-EN4 FLEXI ETHERNET GATEW., SICK FX0-GENT00000 FLEXISOFT EIP GATEW., SICK FX0-GMOD00000 FLEXISOFT MOD GATEW., SICK FX0-GPNT00000 FLEXISOFT PNET GATEW., SICK FX0-GENT00030 FLEXISOFT EIP GATEW.V2, SICK FX0-GPNT00030 FLEXISOFT PNET GATEW.V2 and SICK FX0-GMOD00010 FLEXISOFT MOD GW. have Telnet enabled by factory default. No password is set in the default configuration. Gateways with a serial number >2311xxxx have the Telnet interface disabled by factory default.

- Problem Type:
  - CWE-477
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

6 Additional Resources

[1] Third Party Supplier Advisory:
https://sick.com/.well-known/csaf/white/2023/sca-2023-0002.pdf

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

7 Revision History

28 Apr 2023: Initial Publication