TLP:WHITE

SICK PSIRT
Security Advisory

Use of Telnet in multiple SICK Flexi Soft and Flexi Classic Gateways

Document ID:	SCA-2023-0002
Publication Date:	2023-04-11
CVE Identifier:	CVE-2023-23451
CVSSv3 Base Score:	9.8
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Version:	1

Summary

Several versions of the SICK Flexi Soft Gateways FX0-GENT, FX0-GMOD, FX0-GPNT and SICK Flexi Classic Gateway UE410 provide 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.
Gateways with a serial number >2311xxxx have the Telnet interface disabled by factory default.

List of Products

Product	Part Number	Affected by
SICK FX0-GENT00000 FLEXISOFT EIP GATEW. with serial number <=2311xxxx with Firmware <=V2.11.0	1044072	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK FX0-GENT00030 FLEXISOFT EIP GATEW.V2 with serial number <=2311xxxx all Firmware versions	1099830	CVE-2023-23451 Status: Known Affected Remediation: Mitigation

SICK FX0-GMOD00000 FLEXISOFT MOD GATEW. with serial number <=2311xxxx with Firmware <=V2.11.0	1044073	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK FX0-GMOD00010 FLEXISOFT MOD GW (C) with serial number <=2311xxxx with Firmware <=V2.11.0	1127717	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK FX0-GPNT00000 FLEXISOFT PNET GATEW. with serial number <=2311xxxx with Firmware <=V2.12.0	1044074	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK FX0-GPNT00030 FLEXISOFT PNET GATEW.V2 with serial number <=2311xxxx all Firmware versions	1099832	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK UE410-EN1 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions	1042964	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK UE410-EN3 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions	1042193	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK UE410-EN3S04 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions	1123789	CVE-2023-23451 Status: Known Affected Remediation: Mitigation
SICK UE410-EN4 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions	1044078	CVE-2023-23451 Status: Known Affected Remediation: Mitigation

Vulnerability Overview

CVE-2023-23451 Use of Obsolete Function

Summary: 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.

Description: If the default password is not changed by the operator or customer, a remote unauthorized adversary may connect to the Flexi Soft Gateway via Telnet, interact with the device and change settings of the Gateway. The adversary may also reset the Gateway and in the worst case upload a new firmware version to the device that is then run under root privileges.
SICK recommends to set a strong device individual password once the product is put into operation.

CVE-2023-23451 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-477 (Use of Obsolete Function)

Remediations

Mitigation for CVE-2023-23451

Details: SICK recommends to set a strong password for the Telnet protocol once the Gateway is put into operation. It is possible to set a password with a maximum length of 15 characters.
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 is saved.

Valid for:

- SICK FX0-GENT00000 FLEXISOFT EIP GATEW. with serial number <=2311xxxx with Firmware <=V2.11.0

- SICK FX0-GENT00030 FLEXISOFT EIP GATEW.V2 with serial number <=2311xxxx all Firmware versions
- SICK FX0-GMOD00000 FLEXISOFT MOD GATEW. with serial number <=2311xxxx with Firmware <=V2.11.0
- SICK FX0-GMOD00010 FLEXISOFT MOD GW (C) with serial number <=2311xxxx with Firmware <=V2.11.0
- SICK FX0-GPNT00000 FLEXISOFT PNET GATEW. with serial number <=2311xxxx with Firmware <=V2.12.0
- SICK FX0-GPNT00030 FLEXISOFT PNET GATEW.V2 with serial number <=2311xxxx all Firmware versions
- SICK UE410-EN1 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions
- SICK UE410-EN3 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions
- SICK UE410-EN3S04 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions
- SICK UE410-EN4 FLEXI ETHERNET GATEW. with serial number <=2311xxxx all Firmware versions

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://sick.com/psirt

SICK Operating Guidelines:
https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.PDF

ICS-CERT recommended practices on Industrial Security:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2023-04-11	Initial Release