Security Advisory regarding CVE-2020-10270

We hereby inform that the following products:

Product	*Software version*
MiR100, MiR200, MiR250, MiR500, MiR1000	All
MiR Fleet	All

are affected by:

CVE	*CVSS score*	*Customer risk*
CVE-2020-10270	9.8	High

Overview

MiR products ship with a predefined set of user accounts with default passwords for the web interface.

If the passwords for these accounts are not changed, an attacker in the WiFi network with knowledge of the default credentials could take control of the robot, cause denial of service and exfiltrate data over the web interface.

The emergency stop function provided by the SICK safety PLC is *not* affected.

Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2020-10270

Mitigations

- The Quick Start guide advises all customers to change the default passwords for predefined user accounts of the products' web interface.

Recommended Actions

- Change the default passwords for the predefined user accounts of the products' web interface or remove the accounts if they are not used.