Security Advisory regarding CVE-2020-10274

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-2020-10274	7.1	High

Overview

MiR robots offer a REST-like API to interact with the robot in an automated way, for scenarios where manual use of the web interface is not desired. This API requires authentication using a key derived from user credentials for the web interface.

The credentials of the predefined user accounts for the web interface (see CVE-2020-10270) can be used to access the API.

If the credentials 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-2020-10274

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.
- Please be aware that MiR products must be operated in a secured WiFi network. **An attacker with access to the customer-hosted WiFi network could still exploit this vulnerability.**