Product Security Advisory #006

CVE-2020-10274, CVE-2020-10275

Note
This Product Security Advisory is based on a thorough investigation and all findings that were available at the time of publication. Should new information on the matter become available, it is possible that the initial assessment changes and the Advisory will be updated.

Statement

We hereby inform that the following MiR products:

Product	*Software version*
MiR Robots	All
MiR Fleet	All

are affected by:

CVE	*CVSS score*	*Customer Risk (MiR Score)*
CVE-2020-10274	7.1	High
CVE-2020-10275	9.8	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.

References

- NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10274

- NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10275

Mitigations

- The Cybersecurity Guide advises all customers to change the default passwords for predefined user accounts of the product's web interface or remove the accounts if they are not used.

Recommended Actions

- Change the default passwords for the predefined user accounts of the product's 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.**

Revision history

Date	Description
2022-08-11	Document name and visual update
2021-05-27	Initial Advisory publication