Security Advisory regarding CVE-2020-10272

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-2020-10272	9.8	High

Overview

Two APIs to the Robot Operating System (ROS) used in MiR robots were accessible without authentication.

Using these APIs, an attacker 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-2020-10272

Mitigations

- Starting with software version 2.10.2.1 a firewall prohibits external access to one of the APIs, leaving only the API which is necessary for operation accessible.
- The mitigation of CVE-2020-10269 breaks the chain of attack required to easily exploit this vulnerability over the robot-hosted wireless network.

Recommended Actions

- See Recommended Actions for CVE-2020-10269.
- 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.**