Security Advisory regarding CVE-2020-10269

We hereby inform that the following products:

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

are affected by:

CVE	*CVSS score*	*Customer risk*
CVE-2020-10269	9.8	Critical

Overview

MiR robots shipped before June 2020 were configured with default passwords for their wireless Access Points. This allowed unauthenticated attackers within WiFi range to connect to the wireless networks hosted by MiR robots and access restricted functionality and the internal robot network.

In combination with other flaws, the possible results include loss of control over the robot, denial of service and exfiltrating data stored on the robot (e.g. missions, floor maps).

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

It is important to note that the wireless Access Point is only used during the initial robot setup and should be disabled once no longer needed.

Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2020-10269

Mitigations

- All MiR robots shipped from June 2020 onwards are configured with unique passwords for the WiFi Access Point. Printed paper with the unique password is provided with the robot.

Recommended Actions

- If your robot was shipped before June 2020, change the password for the WiFi Access Point as described in the product service note “Improve the IT security of MiR products” available on the Distributor site.
- The Access Point is only used during the initial setup of the robot. It is strongly recommended to disable the Access Point after the initial robot setup is completed.