Product Security Advisory #002

CVE-2020-10269

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

are affected by:

CVE	*CVSS score*	*Customer Risk (MiR Score)*
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.

References

- NIST NVD entry: 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.

- The User Manual requires users to disable the access point after initial robot setup and instructs how this can be done.

Recommended Actions

- If your robot was shipped before June 2020, change the password for the WiFi Access Point as described in the Cybersecurity Guide available on the MiR Support Portal.

- 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.

Revision history

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