# Product Security Advisory #007

## CVE-2020-10276

**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-2020-10276 | 9.8 | Critical |

### Overview

MiR robots shipped before June 2020 used to have default passwords set for the SICK safety PLC.

**An attacker with access to the internal network of the robot could use the default credentials to manipulate the safety PLC, effectively disabling the emergency stop function.**

This vulnerability is especially critical in combination with CVE-2020-10269, which could be used to gain access to the internal robot network through the robot-hosted wireless network.

### References

NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10276

### Mitigations

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

### Recommended Actions

- If your robot was shipped before June 2020, please change the password for the SICK PLC as described in the product service note “Improve the IT security of MiR products” available on the MiR Support Portal.

## Revision history

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