

Product Security Advisory #003

CVE-2020-10270

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:

<i>Product</i>	<i>Software version</i>
MiR Robots	All
MiR Fleet	All

are affected by:

<i>CVE</i>	<i>CVSS score</i>	<i>Customer Risk (MiR Score)</i>
CVE-2020-10270	9.8	High

Overview

MiR products ship with a predefined set of user accounts with default passwords for the web interface.

If the passwords 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-2020-10270>

Mitigations

- The Cybersecurity Guide advises all customers to either 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.

Revision history

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