

Product Security Advisory #005

CVE-2020-10273

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

are affected by:

<i>CVE</i>	<i>CVSS score</i>	<i>Customer Risk (MiR Score)</i>
CVE-2020-10273	7.5	Low

Overview

MiR robots do not encrypt intellectual property artifacts stored on the robots' hard drives. This means that an attacker with physical access to the hard drive or an attacker with a local account on the robot operating system could extract sensitive data.

It is important to note that the accounts used in the web interface are *not* accounts on the robot operating system. Only MiR support has access to the robot operating system, making this vulnerability relatively difficult to exploit.

In combination with CVE-2020-10269, CVE-2020-10270, CVE-2020-10271 and CVE-2020-10272 certain data can be exfiltrated via the wireless network, should an attacker gain access to it.

References

NIST NVD entry: <https://nvd.nist.gov/vuln/detail/CVE-2020-10273>

Mitigations

- See mitigations for CVE-2020-10269, CVE-2020-10270, CVE-2020-10271 and CVE-2020-10272.
- No additional mitigations: this vulnerability poses a low customer risk. It does not pose a safety hazard, does not influence the operation of MiR robots and cannot be used to compromise the customer's enterprise network.

Recommended Actions

- See Recommended Actions for CVE-2020-10269, CVE-2020-10270, CVE-2020-10271 and CVE-2020-10272.

Revision history

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