Security Advisory regarding CVE-2020-10273

We hereby inform that the following products:

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

are affected by:

CVE	*CVSS score*	*Customer risk*
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.

Link to CVE: 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 enterprise network.

Recommended Actions

- See recommended actions for CVE-2020-10269, CVE-2020-10270, CVE-2020-10271 and CVE-2020-10272.