Product Security Advisory #004

CVE-2020-10271, CVE-2020-10272

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
MiR Fleet	< 3.0.0

are affected by:

CVE	*CVSS score*	*Customer Risk (MiR Score)*
CVE-2020-10271 CVE-2020-10272	9.8	Critical (Robots) High (Fleet)

Overview

Two interfaces to the ROS framework, the ros-master and the ros-bridge, were accessible without authentication from both the wired network interfaces and the robot-hosted wireless access point.

Using these interfaces, an attacker could take control of the robot, cause denial of service and exfiltrate data over the web interface.

The ROS interfaces were *not* exposed to the customer-operated wireless network.

The emergency stop function provided by the SICK safety PLC is *not* affected.

References

NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10271

NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10272

Mitigations

- Starting with software version 2.10.2.1 a firewall prohibits access to the ros-master.
- The mitigation of CVE-2020-10269 (limiting access to the robot-hosted wireless access point) breaks the chain of attack required to easily exploit these vulnerabilities over the robot-hosted wireless network.
- Starting with software version 3 both interfaces are disabled on the MiR Fleet.
- Starting with software version 3 the ros-bridge requires authentication on the MiR Robot.

Recommended Actions

- See Recommended Actions for CVE-2020-10269.
- Upgrade to software version 3.
- Please be aware that MiR products must be operated in a secured WiFi network. **An attacker with access to the customer-hosted WiFi network could still gain access to the ros-bridge on MiR Robots.**

Revision history

Date	Description
2022-08-11	Document name and visual update. Update for SW version 3.
2021-05-27	Initial Advisory publication