Product Security Advisory #008

CVE-2020-10277

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-2020-10277	6.4	Medium

Overview

MiR robots ship with the option to boot from a connected USB drive.

This option is required for some of our customers' use cases and is used by the MiR technical support when a robot needs to be restored. An attacker with physical access to the robot could abuse this functionality to manipulate or exfiltrate data stored on the robot's hard drive.

Booting from USB is enabled by default.

References

NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10277

Mitigations

- USB boot can be disabled in the BIOS. The Cybersecurity Guide contains instructions on how to disable USB boot, should this be desired.

Recommended Actions

- If you wish to disable USB boot, please follow the steps described in the Cybersecurity Guide available on the MiR Support Portal.

Revision history

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