

Product Security Advisory #009

CVE-2020-10278

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-2020-10278	4.6	Medium

Overview

MiR robots ship with no password configured for the BIOS. An attacker with physical access to the robot could manipulate BIOS settings.

References

NIST NVD entry: <https://nvd.nist.gov/vuln/detail/CVE-2020-10278>

Mitigations

- The BIOS can be configured with a password. The Cybersecurity Guide contains instructions on how to configure a BIOS password, should this be desired.

Recommended Actions

- If you wish to configure a BIOS password, 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