Product Security Advisory #010

CVE-2020-10279

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	< 2.8.3
MiR Fleet	< 2.8.3

are affected by:

CVE	*CVSS score*	*Customer Risk (MiR Score)*
CVE-2020-10279	9.8	High

Overview

MiR products used the Ubuntu Server 16.04 LTS operating system. In software versions before 2.8.3 the system was configured with insecure defaults, allowing an authorized local attacker with access to the robot operating system to perform privilege escalation or cause denial of service.

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 for attackers.

Nevertheless, we strongly recommend always keeping MiR software versions up to date, as we continue to provide updates and security patches.

References

NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2020-10279

Mitigations

- Operating system settings are improved, OS has been patched.
- Robot SW version 3 has a new operating system which replaces Ubuntu 16.04.

Recommended Actions

- Install new software versions, especially patches, as provided by MiR. At least software version 2.8.3 is required to mitigate this vulnerability.
- Upgrade to Robot SW version 3.

Revision history

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