Product Security Advisory #001

CVE-2017-7184, CVE-2017-18255

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	< 2.10.2.1
MiR Fleet	< 2.10.2.1

are affected by:

CVE	*CVSS score*	*Customer Risk (MiR Score)*
CVE-2017-7184	7.8	Medium
CVE-2017-18255	7.8	Medium

Overview

An authenticated local attacker with an account on the MiR robot operating system can exploit Linux kernel vulnerabilities to perform privilege escalation to root 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 installing an up-to-date software version in which the vulnerability is removed.

References

- NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2017-7184
- NIST NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2017-18255

Mitigations

- An OS kernel update eliminates the vulnerabilities.

Recommended Actions

- Install new software versions, especially patches, as provided by MiR. To eliminate this vulnerability software version 2.10.2.1 or newer must be installed.

Revision history

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