Security Advisory regarding CVE-2017-7184

We hereby inform that the following products:

Product	*Software version*
MiR100, MiR200, MiR250, MiR500, MiR1000	All before 2.10.2.1
MiR Fleet	All before 2.10.2.1

are affected by:

CVE	*CVSS score*	*Customer risk*
CVE-2017-7184	7.8	Medium

Overview

An authenticated local attacker with an account on the MiR robot operating system can exploit a Linux kernel vulnerability 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.

Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2017-7184

Mitigations

- An OS kernel update eliminates this vulnerability.

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.