Security Advisory regarding CVE-2020-10279

We hereby inform that the following products:

Product	*Software version*
MiR100, MiR200, MiR250, MiR500, MiR1000	All before 2.8.3
MiR Fleet	All before 2.8.3

are affected by:

CVE	*CVSS score*	*Customer risk*
CVE-2020-10279	9.8	High

Overview

MiR products use 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.

Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2020-10279

Mitigations

- Operating system settings are improved, OS has been patched.

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.