Security Advisory regarding CVE-2020-10280

We hereby inform that the following products:

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

are affected by:

CVE	*CVSS score*	*Customer risk*
CVE-2020-10280	7.5	Medium

Overview

An attacker can cause denial of service of the Apache web server by flooding the web interface endpoints with requests.

Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2020-10280

Mitigations

- No mitigations: guarding against such attacks is beyond the capabilities of industrial robots and is much more effectively implemented using network solutions in the IT network of the operator, if such protection is at all desired by the operator.

Recommended Actions

- Please be aware that MiR products must be operated in a secured WiFi network. Consider implementing defense mechanisms against DoS attacks on the network level.