# Product Security Advisory #011

## CVE-2020-10280

**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 | All |
| MiR Fleet | All |

are affected by:

| *CVE* | *CVSS score* | *Customer Risk (MiR Score)* |
|---|---|---|
| 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.

### References

NIST NVD entry: 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.

## Revision history

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