Remediation options for KUNBUS-2025-0000002

This document describes the Options to mitigate the missing authentication in RevPis Node-RED integration in more detail.

Activate authentication

To make access to Node-RED secure, activate access control with a user name and password. To do this, follow the steps below:

1. execute the following command Execute the following command to create a password. The command will prompt you for a password:

```
/usr/share/revpi-nodered/node_modules/node-red/bin/node-red-pi admin hash-pw
```

2. the command returns an encrypted password hash that looks like this:
   $2b$08$abcd1234EfGh...
3. open the file `settings.js`, which is located in the following path:

```
sudo nano /var/lib/revpi-nodered/.node-red/settings.js
```

4. search for the section adminAuth in the file. If this section is missing, add the configuration below to define username and password:

```
adminAuth: {
    type: "credentials",
    users: [{
        username: "admin",
        password: "<HASHED_PASSWORD>",
        permissions: "*"
          }]
},
```

Replace <HASHED_PASSWORD> with the previously generated password hash.

5. Restart the Node-RED service to apply the changes:

```
sudo systemctl restart nodered
```

For more information please have a look at the Node-RED documentation:
https://nodered.org/docs/user-guide/runtime/securing-node-red#usernamepassword-based-authentication

Restrict network access

Make sure that the Node-RED interface is only accessible from trusted networks. Use firewall rules or VLANs to restrict access to the Revolution Pi.

Deactivate unnecessary services

Deactivate Node-RED if not needed. Using the following commands on Commandline e.g. ssh you can stop and disable the Node-RED service.

```
sudo systemctl disable nodered
sudo systemctl stop nodered
```