DOCUMENT ID: SA24P015
VERSION: 1.0
DATE: 2025-03-24

CYBER SECURITY ADVISORY

# B&R APROL
# Potential Privilege Escalation and Information Disclosure

CVE IDs:
CVE-2024-45482, CVE-2024-45481, CVE-2024-45480, CVE-2024-8315, CVE-2024-45484, CVE-2024-45483, CVE-2024-8313, CVE-2024-8314, CVE-2024-10206, CVE-2024-10207, CVE-2024-10208, CVE-2024-10210, CVE-2024-10209

## Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from B&R, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

# Purpose

B&R has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, B&R immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If B&R is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of B&R's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

# Affected products

B&R APROL <4.4-01

# Vulnerabilities IDs

CVE-2024-45482, CVE-2024-45481, CVE-2024-45480, CVE-2024-8315, CVE-2024-45484, CVE-2024-45483, CVE-2024-8313, CVE-2024-8314, CVE-2024-10206, CVE-2024-10207, CVE-2024-10208, CVE-2024-10210, CVE-2024-10209

# Summary

Updates are available that resolve privately reported vulnerabilities in the product versions listed above.

An attacker who successfully exploits these vulnerabilities could elevate privileges or gather sensitive information.

# Recommended immediate actions

The problems are corrected in the following product versions:

| Version | Patched | CVEs |
|---|---|---|
| **B&R APROL 4.4-01** | All versions | CVE-2024-8313<br>CVE-2024-8314<br>CVE-2024-8315<br>CVE-2024-45480<br>CVE-2024-45481<br>CVE-2024-45482<br>CVE-2024-45483<br>CVE-2024-45484<br>CVE-2024-10206<br>CVE-2024-10207<br>CVE-2024-10208<br>CVE-2024-10209<br>CVE-2024-10210 |
| **B&R APROL 4.4-00** | >=4.4-00P1 | CVE-2024-45482 |
| | >=4.4-00P5 | CVE-2024-8313<br>CVE-2024-8314<br>CVE-2024-8315<br>CVE-2024-45480<br>CVE-2024-45481<br>CVE-2024-45482<br>CVE-2024-45484<br>CVE-2024-10206<br>CVE-2024-10207<br>CVE-2024-10208<br>CVE-2024-10210 |

B&R recommends that customers apply the patch or upgrade to a non-vulnerable version at their earliest convenience.

The process to install updates is described in the user manual. The step to identify the installed product version is described in the user manual.

As some of the vulnerabilities affect the confidentiality of credentials, it is recommended to change all secrets/passwords after applying the update.

# Vulnerabilities severity and details

Several vulnerabilities exist in the product versions listed above. An attacker could exploit these vulnerabilities to spoof the identity of legitimate users, gather sensitive information or elevate privileges.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1[1] and v4.0[2].

## CVE-2024-45482 – Privilege escalation in B&R APROL

An Inclusion of Functionality from Untrusted Control Sphere vulnerability in the SSH server on B&R APROL <4.4-00P1 may allow an authenticated local attacker from a trusted remote server to execute malicious commands.

| | |
|---|---|
| CVSS v3.1 Base Score: | 7.8 (High) |
| CVSS v3.1 Temporal Score: | 7.2 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 8.5 (High) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-45482 |

## CVE-2024-45481 – Improper authentication in SSH of B&R APROL

An Incomplete Filtering of Special Elements vulnerability in scripts using the SSH server on B&R APROL <4.4-00P5 may allow an authenticated local attacker to authenticate as another legitimate user.

| | |
|---|---|
| CVSS v3.1 Base Score: | 7.8 (High) |
| CVSS v3.1 Temporal Score: | 7.2 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 8.5 (High) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-45481 |

## CVE-2024-45480 – Unauthorized local file reading in B&R APROL

An improper control of generation of code ('Code Injection') vulnerability in the AprolCreateReport component of B&R APROL <4.4-00P5 may allow an unauthenticated network-based attacker to read files from the local system.

| | |
|---|---|
| CVSS v3.1 Base Score: | 8.6 (High) |

—

[1] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[2] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

| | |
|---|---|
| CVSS v3.1 Temporal Score: | 8.0 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 9.2 (Critical) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-45480 |

### CVE-2024-8315 – Improper Handling of Insufficient Permissions or Privileges in B&R APROL

An Improper Handling of Insufficient Permissions or Privileges vulnerability in scripts used in B&R APROL <4.4-00P5 may allow an authenticated local attacker to read credential information.

| | |
|---|---|
| CVSS v3.1 Base Score: | 5.5 (Medium) |
| CVSS v3.1 Temporal Score: | 5.1 (Medium) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 6.8 (Medium) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-8315 |

### CVE-2024-45484 – Enabled ICMP redirection in B&R APROL

An Allocation of Resources Without Limits or Throttling vulnerability in the operating system network configuration used in B&R APROL <4.4-00P5 may allow an unauthenticated adjacent attacker to perform Denial-of-Service (DoS) attacks against the product.

| | |
|---|---|
| CVSS v3.1 Base Score: | 7.6 (High) |
| CVSS v3.1 Temporal Score: | 7.1 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 7.2 (High) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-45484 |

### CVE-2024-45483 – Missing GRUB password in B&R APROL

A Missing Authentication for Critical Function vulnerability in the GRUB configuration used B&R APROL <4.4-01 may allow an unauthenticated physical attacker to alter the boot configuration of the operating system.

| | |
|---|---|
| CVSS v3.1 Base Score: | 6.8 (Medium) |
| CVSS v3.1 Temporal Score: | 6.3 (Medium) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 7.0 (Medium) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-45483 |

### CVE-2024-8313 – Default or Guessable SNMP community names in B&R APROL

An Exposure of Sensitive System Information to an Unauthorized Control Sphere and Initialization of a Resource with an Insecure Default vulnerability in the SNMP component of B&R APROL <4.4-00P5 may allow an unauthenticated adjacent-based attacker to read and alter configuration using SNMP.

| | |
|---|---|
| CVSS v3.1 Base Score: | 8.8 (High) |
| CVSS v3.1 Temporal Score: | 8.2 (Medium) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C |
| | |
| CVSS v4.0 Score | 8.7 (High) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| | |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-8313 |

### CVE-2024-8314 – Improper session handling in B&R APROL

An Incorrect Implementation of Authentication Algorithm and Exposure of Data Element to Wrong Session vulnerability in the session handling used in B&R APROL <4.4-00P5 may allow an authenticated network attacker to take over a currently active user session without login credentials.

| | |
|---|---|
| CVSS v3.1 Base Score: | 8.0 (High) |
| CVSS v3.1 Temporal Score: | 7.4 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C |
| | |
| CVSS v4.0 Score | 5.5 (Medium) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H |
| | |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-8314 |

### CVE-2024-10206 – Server-Side Request Forgery (unauthenticated) in APROL Web Portal

A Server-Side Request Forgery vulnerability in the APROL Web Portal used in B&R APROL <4.4-00P5 may allow an unauthenticated network-based attacker to force the web server to request arbitrary URLs.

| | |
|---|---|
| CVSS v3.1 Base Score: | 5.3 (Medium) |
| CVSS v3.1 Temporal Score: | 4.9 (Medium) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C |
| | |
| CVSS v4.0 Score | 6.9 (Medium) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N |
| | |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-10206 |

### CVE-2024-10207 – Server-Side Request Forgery (authenticated) in APROL Web Portal

A Server-Side Request Forgery vulnerability in the APROL Web Portal used in B&R APROL <4.4-00P5 may allow an authenticated network-based attacker to force the web server to request arbitrary URLs

| | |
|---|---|
| CVSS v3.1 Base Score: | 4.3 (Medium) |
| CVSS v3.1 Temporal Score: | 4.0 (Medium) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C |
| | |
| CVSS v4.0 Score | 5.3 (Medium) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N |

| | |
|---|---|
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-10207 |

### CVE-2024-10208 – Cross Site Scripting vulnerability in APROL Web Portal

An Improper Neutralization of Input During Web Page Generation vulnerability in the APROL Web Portal used in B&R APROL <4.4-00P5 may allow an authenticated network-based attacker to insert malicious code which is then executed in the context of the user's browser session.

| | |
|---|---|
| CVSS v3.1 Base Score: | 6.1 (Medium) |
| CVSS v3.1 Temporal Score: | 5.7 (Medium) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 5.1 (Medium) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-10208 |

### CVE-2024-10210 – Path traversal in APROL Web Portal

An External Control of File Name or Path vulnerability in the APROL Web Portal used in B&R APROL <4.4-005P may allow an authenticated network-based attacker to access data from the file system.

| | |
|---|---|
| CVSS v3.1 Base Score: | 8.5 (High) |
| CVSS v3.1 Temporal Score: | 7.9 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 8.4 (High) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:H/SI:L/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-10210 |

### CVE-2024-10209 – Incorrect Permission Assignment in APROL file system

An Incorrect Permission Assignment for Critical Resource vulnerability in the file system used in B&R APROL <4.4-01 may allow an authenticated local attacker to read and alter the configuration of another engineering or runtime user.

| | |
|---|---|
| CVSS v3.1 Base Score: | 7.8 (High) |
| CVSS v3.1 Temporal Score: | 7.2 (High) |
| CVSS v3.1 Vector: | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C |
| CVSS v4.0 Score | 8.5 (High) |
| CVSS v4.0 Vector: | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| NVD Summary Link: | https://nvd.nist.gov/vuln/detail/CVE-2024-10209 |

## Mitigating factors

Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed. Please refer to "General security recommendations" to get general guidelines how to mitigate threats on IACS.

B&R can support customers with various measures to mitigate the listed vulnerabilities. Please contact APROL Support for assistance.

# Frequently asked questions

### What causes the vulnerabilities?

The vulnerabilities are caused by various security flaws in the impacted product versions. Please refer to the CWE numbers mentioned in the vulnerability descriptions on NVD for more details.

### What is B&R APROL?

B&R APROL is an industrial control system, which was developed as a homogeneous, integrated complete system. Central engineering with a global engineering database allows completely consistent automation

### What might an attacker use the vulnerabilities to do?

An attacker might:

- insert malicious code or execute commands
- cause information disclosure, including sensitive information
- to read and alter configuration information
- take over a currently active user session
- force the product to request arbitrary URLs
- cause denial of service conditions

### Could the vulnerabilities be exploited remotely?

For information on whether an individual vulnerability can also be exploited remotely, please refer to the detailed vulnerability description

Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed

### What does the update do?

The update removes the vulnerability by modifying the way that the B&R APROL uses file permissions, removes unintended functionalities, hardens authentication mechanisms, and how environmental variables are defined.

### When this security advisory was issued, had this vulnerability been publicly disclosed?

No, B&R received information about this vulnerability through responsible disclosure

### When this security advisory was issued, had B&R received any reports that this vulnerability was being exploited?

No, B&R had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

# General security recommendations

For any installation of software-related B&R products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following documents:

Defense in Depth for B&R products

# Support

For additional instructions and support please contact your local B&R service organization. For contact information, see https://www.br-automation.com/en/about-us/locations/.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

# Version history

| Rev. Ind. | Page (p) Chapter (c) | Change description | Version. date |
|---|---|---|---|
| 1.0 | all | Initial version | 2025-03-24 |
| | | | |
| | | | |