DOCUMENT ID: SA24P014
VERSION: 1.1
DATE: 2024-08-28

CYBER SECURITY ADVISORY

B&R APROL
Multiple vulnerabilities in B&R APROL

CVE IDs: CVE-2024-5622, CVE-2024-5623, CVE-2024-5624

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.

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

Product Name	Issue	Affected versions
B&R APROL	CVE-2024-5622	<= R 4.2-07P3
		<= R 4.4-00P3
	CVE-2024-5623 CVE-2024-5624	<= R 4.4-00P3

Vulnerability IDs

CVE-2024-5622, CVE-2024-5623, CVE-2024-5624

Summary

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

An attacker who successfully exploited the vulnerabilities could insert and run arbitrary code with elevated privileges or construct a hyperlink that, if issued by another user, could execute malicious script code in the context of the user's browser session.

Recommended immediate actions

The problem is corrected in the following product versions:

Product Name	Version line	Issues	Patched version
B&R APROL	4.2	CVE-2024-5622	>= R 4.2-07P4
		CVE-2024-5623 CVE-2024-5624	Pending
	4.4	CVE-2024-5622 CVE-2024-5623 CVE-2024-5624	>= R 4.4-00P4

B&R recommends that customers apply the update at 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.

Vulnerability severity and details

Some vulnerabilities exist in the underlying operating system configuration and the Web application included in the product versions listed above. An attacker who successfully exploited the vulnerabilities could insert and run arbitrary code with elevated privileges, or construct a hyperlink that, if issued by another user, could execute malicious script code in the context of the user's browser session.

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-2024-5622

An untrusted search path vulnerability in the AprolConfigureCCServices of B&R APROL <= R 4.2-07P3 and <= R 4.4-00P3 may allow an authenticated local attacker to execute arbitrary code with elevated privileges.

CVSS v3.1 Base Score: 7.8 (High)
CVSS v3.1 Temporal Score: 6.8 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v4.0 Score 7.3 (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 v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:P/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-2024-5622

CVE-2024-5623

An untrusted search path vulnerability in B&R APROL <= R 4.4-00P3 may be used by an authenticated local attacker to get other users to execute arbitrary code under their privileges.

CVSS v3.1 Base Score: 7.3 (High)
CVSS v3.1 Temporal Score: 6.4 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v4.0 Score 5.4 (Medium)
CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-5623

CVE-2024-5624

Reflected Cross-Site Scripting (XSS) in Shift Logbook application of B&R APROL <= R 4.4-00P3 may allow a network-based attacker to execute arbitrary JavaScript code in the context of the user's browser session.

CVSS v3.1 Base Score: 6.1 (Medium)
CVSS v3.1 Temporal Score: 5.3 (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:U/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-2024-5624

Workarounds and mitigating factors

Do not use hyperlinks provided by untrusted 3 rd party to access the Shift Logbook application. Hyperlinks may be provided via:

- Emails from unknown users
- Social media channels
- Messaging services
- Webpages with comment functionality
- QR Codes

The use of external Web Application Firewalls (WAF) can mitigate attacks using reflected cross-site scripting.

To exploit the vulnerabilities CVE-2024-5623 and CVE-2024-5622, access with a low privileged account to the APROL system is required. In general, limit any kind of access to the APROL system to trusted persons.

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

What causes the vulnerabilities?

CVE Number	Exploitation example
CVE-2024-5622 **CVE-2024-5623**	The vulnerabilities are caused by insufficient handling of search paths in B&R APROL.
CVE-2024-5624	The vulnerability is caused by improper neutralization of input during Web page generation in B&R APROL.

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 vulnerability to do?

CVE Number	Exploitation example
CVE-2024-5622 **CVE-2024-5623**	An attacker who successfully exploited the vulnerabilities could insert and run arbitrary code.
CVE-2024-5624	An attacker who successfully exploited the vulnerability could execute malicious script code in the context of the user's browser session.

How could an attacker exploit the vulnerability?

CVE Number	Exploitation example
CVE-2024-5622 **CVE-2024-5623**	An attacker could try to exploit the vulnerabilities by creating a specially crafted malicious script and executing the script with higher privileges on a system node.
CVE-2024-5624	An attacker could construct a hyperlink that, if clicked by another user, could execute malicious script code in the context of the user's browser session.

Could the vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities. 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 vulnerabilities by modifying how the B&R APROL uses file permissions, environment variables, and performs input sanitization.

When this security advisory was issued, had these vulnerabilities been publicly disclosed?

No, B&R received information about these vulnerabilities through responsible disclosure.

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

No, B&R had not received any information indicating that these vulnerabilities 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.

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	2024-08-27
1.1	p2-4	Fixing mistyped CVE numbers, improved CVE description in terms of versioning	2024-08-28