DOCUMENT ID: SA22P016
VERSION: 1.1
DATE: 2023-02-03

CYBER SECURITY ADVISORY

B&R APROL
Several Issues in APROL database

CVE ID: CVE-2022-43761, CVE-2022-43762, CVE-2022-43763, CVE-2022-43764, CVE-2022-43765

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

B&R APROL < R 4.2-07

Vulnerability IDs

CVE-2022-43761, CVE-2022-43762, CVE-2022-43763, CVE-2022-43764, CVE-2022-43765

Summary

B&R is aware of several issues in the APROL database of all B&R APROL versions listed above. An attacker may use these vulnerabilities to cause Denial of Service conditions or harm the integrity and confidentiality of data.

Recommended immediate actions

B&R offers an update that allows the customer to restrict access to the affected component by using TLS Client Authentication (Mutual TLS).

The mitigation option is available in APROL version >= R 4.2-07 with AutoYaST >=V4.2-070.0.120102. 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

Several vulnerabilities exist in the APROL database included in the product versions listed above. An attacker could exploit the vulnerabilities by sending a specially formatted message to the affected component which could cause a Denial of Service condition, execute of arbitrary code or harm the integrity and confidentiality of configuration data.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2022-43761 Lack of authentication when managing APROL database

Missing authentication when creating and managing the APROL database allows changing the system configuration.

CVSS v3.1 Base Score:	9.4
CVSS v3.1 Temporal Score:	8.7
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:F/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-43761

CVE-2022-43762 Memory leak when receiving messages in APROL Tbase server

Lack of verification in APROL Tbase server may lead to memory leaks when receiving messages.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	7.0
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:T/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-43762

CVE-2022-43763 Lack of checking preconditions in APROL

Insufficient check of preconditions could lead to Denial of Service conditions when calling commands on the Tbase server.

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	7.3
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:U/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-43763

CVE-2022-43764 Buffer overflow when changing configuration on Tbase server

Insufficient validation of input parameters when changing configuration on Tbase server in B&R APROL could result in buffer overflow. This may lead to Denial-of-Service conditions or execution of arbitrary code.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	9.2

[1] 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.

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:T/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-43764

CVE-2022-43765 DoS in APROLs Tbase server

APROL doesn't process correctly specially formatted data packages sent to port 55502/tcp, which may allow a network based attacker to cause an application Denial-of-Service.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Temporal Score: 7.0
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:T/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-43765

Mitigating factors

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

Workarounds

B&R has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can limit attack vectors.

B&R recommends using the Linux firewall to limit accessibility of TCP port 55502. Grant access only to trusted IP addresses or specific IP address ranges. Make sure only trusted users can connect their devices to the specified IP range.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploit these vulnerabilities could remotely cause an affected system node to stop or insert and run arbitrary code in an affected system node.

What causes the vulnerability?

CVE-2022-43761: The vulnerability is caused by incomplete user authentication in the Tbase server in B&R APROL

CVE-2022-43765, CVE-2022-43764, CVE-2022-43762: The vulnerability is caused by insufficient input validation in the Tbase server in B&R APROL

CVE-2022-43763: The vulnerability is caused by insufficient check of preconditions in the Tbase server in B&R APROL

What is APROL?

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-2022-43761: An attacker who successfully exploit this vulnerability could change or read the configuration or cause the affected node to stop operating.

CVE-2022-43765: An attacker who successfully exploit this vulnerability could read data from the affected system node.

CVE-2022-43764, CVE-2022-43763: An attacker who successfully exploit this vulnerability could cause the affected system node to stop or become inaccessible

CVE-2022-43762: An attacker who successfully exploit this vulnerability could insert and run arbitrary code in the context of the affected system node.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that the attacker installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigating such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker with network access to an affected system node could exploit this vulnerability. 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 e.g. a firewall system that has a minimal number of ports exposed.

What does the update do?

The update mitigates the vulnerability by giving the possibility to restrict access to the vulnerable component using Mutual TLS (Client Authentication).

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.

Acknowledgement

B&R thanks Nataliya Tlyapova from Positive Technologies for helping us to keep our products secure.

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	2023-01-30
1.1	Title	Corrected typing in title	2023-02-03